นโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

โดย

นายไตรรัตน์ วิริยะศิริกุล
รองเลขาธิการ กสทช. รักษาการแทน เลขาธิการ กสทช.
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์
และกิจการโทรคมนาคมแห่งชาติ

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕
ประจำปีการศึกษา พุทธศักราช ๒๕๖๕ - ๒๕๖๖

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “นโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่” ลักษณะวิชา สังคมจิตวิทยา ของนายไตรรัตน์ วิริยะศิริกุล รองเลขาธิการ กสทช. รักษาการแทน เลขาธิการ กสทช. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕ ประจำปีการศึกษา พุทธศักราช ๒๕๖๕ – ๒๕๖๖

พลโท

(พลโท ชาติชาย ชัยเกษม)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง นโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

ลักษณะวิชา สังคมจิตวิทยา

ผู้วิจัย นายไตรรัตน์ วิริยะศิริกุล **หลักสูตร** วปอ. **รุ่นที่** ๖๕

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่หรือแก๊งคอลเซ็นเตอร์ (Call Center) ถือเป็นอาชญากรรมทางสังคมร้ายแรง ซึ่งส่งผลกระทบกับประชาชนและความมั่นคงของประเทศในปัจจุบัน เอกสารวิจัยส่วนบุคคล เรื่อง “นโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่” จึงมีจุดประสงค์หลักเพื่อศึกษาพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ผลกระทบและแนวทางการดำเนินการในการแก้ไขหรือป้องกันในปัจจุบัน เพื่อให้สามารถนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาในประเทศไทยแบบบูรณาการ งานวิจัยชิ้นนี้มีขอบเขตด้านเนื้อหาคือมุ่งเน้นการศึกษาเฉพาะพฤติกรรมที่เกิดขึ้นกับกลุ่มบุคคลทั่วไป และมีขอบเขตด้านประชากรคือมีกลุ่มเป้าหมายที่จะดำเนินการเก็บข้อมูลผ่านการสัมภาษณ์เชิงลึกงานวิจัยชิ้นนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ โดยดำเนินการทั้งการศึกษาเอกสาร (Documentary Research)และการสัมภาษณ์เชิงลึก (In-depth interview) กับผู้เชี่ยวชาญที่มีความรู้ความเข้าใจกับปัญหารวมทั้งสิ้น ๖ ท่าน

จากการวิเคราะห์ข้อมูลด้วยการวิเคราะห์ช่องว่าง (Gap Analysis) และใช้ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ผลการวิจัยพบว่า การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มีลักษณะที่สำคัญหลายประการ ได้แก่ มิจฉาชีพมีการทำงานเป็นกลุ่มขบวนการ มีการตั้งฐานปฏิบัติการในต่างประเทศและมีลักษณะเหมือนอาชญากรรมข้ามชาติ สามารถจัดหาช่องทางและอุปกรณ์ต่าง ๆ ที่ใช้ในการสื่อสารเพื่อเข้าถึงเป้าหมายได้หลายวิธี ใช้หลักการหลอกลวงทางจิตวิทยาต่าง ๆ เพื่อโจมตีจุดอ่อนของเป้าหมาย และมีการใช้ Mobile Banking และบัญชีม้าในการโยกย้ายทรัพย์สิน การหลอกลวงดังกล่าวสร้างผลกระทบเป็นอย่างมากต่อความอยู่ดีมีสุขของประชาชน ผู้ประกอบการและหน่วยงานที่เกี่ยวข้องสังคมประเทศและความมั่นคง การดำเนินการในปัจจุบันพบว่ามีการดำเนินการที่ครอบคลุมทั้ง ๓ ส่วนของทฤษฎีสามเหลี่ยมอาชญากรรม คือ ผู้กระทำผิด ผู้เสียหาย โอกาสและช่องทางของการกระทำผิดและมีการแก้ไขปัญหาในภาพรวม เช่น การบังคับใช้ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี อย่างไรก็ดี เพื่อให้สามารถแก้ไขและป้องกันปัญหาการหลอกลวงในประเทศไทยได้อย่างมีประสิทธิภาพ งานวิจัยนี้จึงนำเสนอข้อเสนอแนะเชิงนโยบายที่มุ่งเน้นให้มีการปรับแก้กฎหมายให้มีความเหมาะสมและบังคับใช้กฎหมายที่มีให้เกิดประโยชน์สูงสุด และข้อเสนอแนะเชิงปฏิบัติการที่มุ่งเน้นการเยียวยาผู้เสียหายโดยเฉพาะด้านจิตใจ และการปกป้องประชาชนจากมิจฉาชีพทั้งการสร้างความตระหนักรู้ การใช้ระบบแจ้งเตือนที่นำเทคโนโลยีการใหม่ ๆ มาใช้ และจัดตั้งความร่วมมือของหน่วยงานต่าง ๆ แบบบูรณาการ

Abstract

Title Policies and measures to eradicate and prevent issues regarding scams via mobile phone network

Field Social - Psychology

Name Mr. Trairat Viriyasirikul **Course** NDC **Class** 65

Scams via mobile phone network issues are considered as a severe social crime affecting people and national security recently. This individual research entitled “Policies and measures to eradicate and prevent issues regarding scams via mobile phone network” aims to study the behaviors of scammers, its impacts, and incumbent policies and measures implemented to solve and prevent such issues nowadays. The results are used to establish integrated policy recommendations and measures to eradicate the problem in Thailand. Regarding the scope of the study, it includes the issues occurring in the individuals. Target group, as demographic scope, are experts in the field. This research adopts qualitative methodology comprising of documentary research, and in-depth interviews conducted on total six experts relating to the issues.

The data were analyzed by gap analysis based on crime triangle theory. The results found that mobile phone network scams have several important characteristics; the scammers have bases of operations overseas, similar to transnational crime; they use various communication means and devices to reach the target; they employ psychological methods to deceive and attack the target's weaknesses, and they use mobile banking and mule accounts to migrate assets to their accounts. These issues immensely affect people’s well-being, society, the country, and the national security. Existing policies and measures cover all the factors included in the crime triangle theory, the offenders, victims/targets and opportunity/place, and also measures intended to solve the problem as a whole. For example, the Royal Decree on Measures for Protection and Suppression of Technology Crime B.E. 2566 has been enacted. Nonetheless, in order to effectively eradicate and prevent these issues in Thailand, this research proposes several appropriate recommendations. The policy recommendations focus on amending and enforcing the law. The operational recommendations include victim support, especially psychologically, protecting people from scammers such as raising awareness, usage of a notification system utilizing new technologies and establishing an integrated cooperation of various relevant agencies.

คำนำ

ในปัจจุบันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ หรือที่เรียกกันว่าแก๊งคอลเซ็นเตอร์ (Call Center) ถือเป็นอาชญากรรมทางสังคมที่สำคัญ ส่งผลกระทบกับประชาชน สังคม และความมั่นคงในวงกว้าง มิจฉาชีพได้อาศัยช่องทางการสื่อสารเป็นหลักในการหลอกลวง เพื่อทำให้ประชาชนหลงเชื่อและทำให้ต้องสูญเสียทั้งข้อมูลส่วนตัวและทรัพย์สินของตัวเอง หน่วยงานภาครัฐที่เกี่ยวข้อง ทั้งในด้านการเงินการธนาคาร ด้านความมั่นคง รวมทั้งด้านการสื่อสารโทรคมนาคม ต่างพยายามร่วมมือกันในการแก้ไขและป้องกันปัญหาดังกล่าวมาโดยตลอด อย่างไรก็ตาม มิจฉาชีพได้มีการพัฒนารูปแบบวิธีการหลอกลวงไปเรื่อย ๆ ทำให้หน่วยงานต่าง ๆ ต่างต้องพยายามพัฒนาแนวทางเพื่อให้สามารถแก้ไขและป้องกันปัญหาแก๊งคอลเซ็นเตอร์และการหลอกลวงอื่น ๆ ได้ทันต่อสถานการณ์

งานวิจัยฉบับนี้ได้มีการศึกษาแนวคิด ทฤษฎี และวรรณกรรมต่าง ๆ เพื่อให้เข้าใจถึงลักษณะที่มาของปัญหาทั้งจากผู้กระทำผิดและผู้ตกเป็นเป้าหมาย ผลกระทบของปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ตลอดจนได้ศึกษาและรวบรวมข้อมูลการดำเนินการที่เกิดขึ้นจริงภายในประเทศในการแก้ไขและป้องกันปัญหาการหลอกลวงดังกล่าวจากผู้แทนหน่วยงานภาครัฐที่เกี่ยวข้องและผู้ให้บริการโทรศัพท์เคลื่อนที่ภาคเอกชน รวมทั้งศึกษาข้อมูลการดำเนินการในต่างประเทศเพื่อนำมาประยุกต์ใช้ในงานวิจัยชิ้นนี้ และจัดทำข้อเสนอแนะแนวทางการดำเนินการเพิ่มเติมทั้งในเชิงนโยบายและเชิงมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย ด้วยความมุ่งมั่นที่ต้องการจะลดความเสียหายที่เกิดขึ้นกับประชาชนจากปัญหาการหลอกลวงดังกล่าวทั้งทางด้านจิตใจและทรัพย์สิน ตลอดจนความเสียหายที่เกิดขึ้นกับสังคม

ผู้วิจัยหวังเป็นอย่างยิ่งว่างานวิจัยฉบับนี้จะเป็นประโยชน์และสามารถนำไปประยุกต์ใช้เป็นแนวทางเพิ่มเติมในการการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย เพื่อให้เกิดประโยชน์ตามที่คาดหวังในการลดผลกระทบหรือความเสียหายที่เกิดขึ้นต่อประชาชน สังคม เศรษฐกิจ และความมั่นคงของประเทศ ซึ่งจะช่วยให้บรรลุยุทธศาสตร์ชาติ ที่มีเป้าหมายสำคัญในภาพรวมระยะ ๒๐ ปี คือ “ประเทศชาติมั่นคง ประชาชนมีความสุข” ต่อไป

(นายไตรรัตน์ วิริยะศิริกุล)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๕
ผู้วิจัย

กิตติกรรมประกาศ

งานวิจัยฉบับนี้สำเร็จลงได้ด้วยดี ต้องขอขอบพระคุณอาจารย์ที่ปรึกษา พล.อ. ราเมศร์ สันติบุตร ที่ให้ความกรุณาอย่างสูงในการให้คำแนะนำและคำปรึกษาที่เป็นประโยชน์อย่างยิ่ง ขอขอบคุณเจ้าหน้าที่กองเอกสารวิจัยและห้องสมุด วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ที่ให้ความกรุณาตรวจสอบและให้คำแนะนำในการปรับปรุงแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่อย่างดียิ่ง

ขอขอบคุณผู้แทนกองบังคับคดีการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ผู้แทนธนาคารแห่งประเทศไทย ผู้แทนจากบริษัทผู้ประกอบกิจการที่เกี่ยวข้อง และผู้แทนจากสำนักงาน กสทช. ที่ให้โอกาสในการสัมภาษณ์เพื่อรวบรวมข้อมูลข้อเท็จจริง รวมทั้งให้ความเห็นและข้อเสนอแนะต่าง ๆ อันเป็นประโยชน์อย่างยิ่งในการจัดทำงานวิจัยฉบับนี้

ผู้วิจัยหวังเป็นอย่างยิ่งว่างานวิจัยฉบับนี้จะเป็นประโยชน์ต่อสังคมไทยในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย หากงานวิจัยฉบับนี้มีความผิดพลาดประการใด ผู้วิจัยขอน้อมรับไว้แต่เพียงผู้เดียว

(นายไตรรัตน์ วิริยะศิริกุล)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๕
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ยุทธศาสตร์ชาติด้านความมั่นคงกำหนดให้บริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคงปลอดภัย และมีความสงบเรียบร้อยในทุกระดับตั้งแต่ระดับชาติสังคม ชุมชน ไปจนถึงระดับความมั่นคงของมนุษย์และทุกมิติให้มีความพร้อมสามารถรับมือกับภัยคุกคามและภัยพิบัติได้ทุกรูปแบบโดยใช้กลไกการแก้ไขปัญหาแบบบูรณาการทั้งกับส่วนราชการ ภาคเอกชน ประชาสังคม เพื่อสนับสนุนกรอบแนวคิด “ความมั่นคงแบบองค์รวม” และสามารถบรรลุเป้าหมายสำคัญในภาพรวมระยะ ๒๐ ปี คือ “ประเทศชาติมั่นคง ประชาชนมีความสุข” ได้อย่างเป็นรูปธรรม อย่างไรก็ดีเป็นที่ทราบกันโดยทั่วไปว่าปัจจุบัน**ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่โดยเฉพาะอย่างยิ่งภัยการหลอกลวงทางโทรศัพท์ มิจฉาชีพคอลเซ็นเตอร์ หรือแก๊งคอลเซ็นเตอร์ (Call Center)** ถือเป็นอาชญากรรมทางสังคมที่สำคัญซึ่งส่งผลกระทบกับประชาชนและความมั่นคงในวงกว้าง มีประชาชนจำนวนมากถูกหลอกลวงและสูญเสียทรัพย์สิน โดยมิจฉาชีพได้อาศัยช่องทางการสื่อสารทำการหลอกลวงทั้งการโทร การส่งข้อความผ่านบริการส่งข้อความสั้น (SMS) และการหลอกลวงผ่านช่องทางออนไลน์โดยเฉพาะสื่อโซเชียลมีเดียต่าง ๆ และมีการพัฒนารูปแบบวิธีการหลอกลวงไปเรื่อย ๆ เพื่อสร้างความน่าเชื่อถือ สร้างความหวาดกลัว และชักจูงใจด้วยวิธีต่าง ๆ เพื่อทำให้ประชาชนหลงเชื่อและทำให้ต้องสูญเสียทั้งข้อมูลส่วนตัวและทรัพย์สินของตัวเอง โดยตามรายงานจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศพบว่า ประเทศไทยมีการใช้โทรศัพท์เพื่อหลอกลวงมากกว่า ๖.๔ ล้านครั้ง โดยเพิ่มขึ้นกว่าร้อยละ ๒๗๐ จากปี ๒๕๖๓ และพบการส่งข้อความสั้น (SMS) หลอกลวงเพิ่มขึ้นถึงร้อยละ ๕๗ นอกจากนี้ในปี ๒๕๖๔ ที่ผ่านมามีผู้เสียหายเข้าแจ้งความกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กว่า ๑,๖๐๐ ราย มูลค่าความเสียหายสูงกว่า ๑,๐๐๐ ล้านบาท (สำนักงานเลขาธิการสภาผู้แทนราษฎร, ๒๕๖๕) สำหรับในส่วนของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) เองนั้นก็ได้มีการรวบรวมสถิติการแจ้งเบาะแสและปัญหาเกี่ยวกับกรณีการหลอกลวงผ่านช่องทางโทรศัพท์ (Call Center) และข้อความสั้น (SMS) เฉพาะที่มีการแจ้งมายังสำนักงาน กสทช. ผ่าน Call Center ๑๒๐๐ โดยในปี ๒๕๖๔ มีการแจ้งเรื่องร้องเรียนโทรศัพท์ (Call Center) และข้อความสั้น (SMS) ที่อาจเข้าข่ายหลอกลวงเป็นจำนวน ๓๔๒ ราย และแจ้งเบาะแสเป็นจำนวน ๙๕๖ ราย ส่วนในปี ๒๕๖๕ (ข้อมูล ณ สิ้นไตรมาสที่ ๒) มีการแจ้งเรื่องร้องเรียนเป็นจำนวน ๒๗๙ ราย และแจ้งเบาะแสเป็นจำนวน ๖๔๓ ราย รูปแบบที่มากที่สุดได้แก่ การอ้างเป็นเจ้าหน้าที่ของรัฐ (เช่น ตำรวจ สำนักงาน กสทช. กรมสรรพากร กรมสอบสวนคดีพิเศษ) เพื่อหลอกลวงว่ามีการทำผิดกฎหมายต้องจ่ายค่าปรับหรือโอนเงินให้เพื่อตรวจสอบบัญชี การแจ้งจะระงับบริการโทรศัพท์เคลื่อนที่ การอ้างว่ามีการตรวจสอบพบว่ามีการหลบเลี่ยงการจ่ายภาษี หรือการแจ้งให้ติดตั้งโปรแกรมที่ปิดกั้นการ

หลอกลวงได้ทั้งหมด รองลงมา ได้แก่ การอ้างเรื่องสินเชื่อเงินกู้ โดยแจ้งว่าได้รับวงเงินสินเชื่อจำนวนมาก ตั้งแต่ ๑๐๐,๐๐๐ - ๒๐๐,๐๐๐ บาท และการอ้างเป็นพนักงานส่งพัสดุโดยแจ้งว่ามีพัสดุตกค้างที่อาจผิดกฎหมายต้องมีการยืนยันและชำระเงิน

สำนักงาน กสทช. ในฐานะหน่วยงานหลักในการกำกับดูแลกิจการโทรคมนาคมได้ตระหนักถึงภัยจากการหลอกลวงดังกล่าว จึงได้มีการแต่งตั้งคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งค์โทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง โดยมีผู้แทนภาคส่วนต่าง ๆ ที่เกี่ยวข้องทั้งภาครัฐและเอกชน ได้แก่ ผู้แทนปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผู้แทนคณะกรรมการข้อมูลส่วนบุคคล ผู้แทนธนาคารแห่งประเทศไทย ผู้แทนกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ผู้แทนบริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด ผู้แทนบริษัท ดีแทค ไตรเน็ต จำกัด ผู้แทนบริษัท ทรู มูฟ เอช ยูนิเวอร์แซล คอมมิวนิเคชั่น จำกัด ผู้แทนบริษัท โทรคมนาคมแห่งชาติ จำกัด ผู้แทนสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ ผู้แทนสภาองค์กรผู้บริโภค และผู้แทนจากสำนักงาน กสทช. เพื่อศึกษาวิเคราะห์มาตรการ และข้อกฎหมายต่าง ๆ ที่เกี่ยวข้องในการแก้ปัญหาแก๊งค์โทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง และสร้างช่องทางเพื่อรับแจ้งปัญหาระหว่างหน่วยงานและใช้เป็นฐานข้อมูลสำหรับสำนักงาน กสทช. ในการให้ความรู้แก่ผู้บริโภค รวมถึงออกแบบกระบวนการในการแก้ปัญหา

ดังนั้น จะเห็นได้ว่าปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่หรือแก๊งคอลเซ็นเตอร์ (Call Center) ถือเป็นภัยทางสังคมระดับชาติและเป็นภัยต่อความมั่นคงของประเทศ เพื่อลดความเสียหายที่เกิดขึ้นกับประชาชนจากปัญหาการหลอกลวงดังกล่าวจึงมีความจำเป็นที่จะต้องจัดทำงานวิจัยฉบับนี้เพื่อศึกษาปัญหาดังกล่าวโดยละเอียดตั้งแต่พฤติกรรมในการหลอกลวงและผลกระทบที่เกิดขึ้นต่อสังคมและผู้บริโภค แนวทางการดำเนินการในการแก้ไขหรือป้องกันการหลอกลวง เพื่อ**นำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ** ทั้งในส่วนของหน่วยงานภาครัฐที่เกี่ยวข้อง ผู้ให้บริการโทรศัพท์เคลื่อนที่ ผู้ให้บริการโทรคมนาคมที่เกี่ยวข้อง และผู้บริโภค

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ และผลกระทบที่เกิดขึ้นต่อสังคมและผู้บริโภค

๒. เพื่อศึกษาแนวทางการดำเนินการในการแก้ไขหรือป้องกันการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในปัจจุบัน

๓. เพื่อนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

ขอบเขตของการวิจัย

๑. ขอบเขตด้านเนื้อหา

การวิจัยนี้มุ่งเน้นการศึกษาเฉพาะพฤติกรรมที่เกิดขึ้นในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในส่วนที่เกิดขึ้นกับกลุ่มบุคคลทั่วไปและแนวทางการดำเนินการของหน่วยงานที่เกี่ยวข้องในการแก้ไขหรือป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ เพื่อนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

๒. ขอบเขตด้านประชากร

กลุ่มเป้าหมายที่จะดำเนินการเก็บข้อมูลผ่านการสัมภาษณ์เชิงลึก (In-depth Interview) แบ่งออกเป็น ๒ กลุ่มคือ

๒.๑ เจ้าหน้าที่ตำรวจ

๒.๒ ผู้แทนในคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งค์โทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง

วิธีดำเนินการวิจัย

งานวิจัยเรื่อง ข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ ผู้วิจัยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยดำเนินการ ดังนี้

๑. การรวบรวมข้อมูล

๑.๑ เครื่องมือในการรวบรวมข้อมูล

๑.๑.๑ การศึกษาเอกสาร (Documentary Research)

ผู้วิจัยจะดำเนินการศึกษาข้อมูลทุติยภูมิผ่านเอกสารที่เกี่ยวข้องกับรูปแบบและพฤติกรรมการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่และการดำเนินมาตรการในการแก้ไขและป้องกันปัญหาดังกล่าวทั้งในประเทศและต่างประเทศ

๑.๑.๒ การสัมภาษณ์เชิงลึก (In-depth Interview)

ผู้วิจัยจะดำเนินการศึกษาข้อมูลปฐมภูมิผ่านการสัมภาษณ์เชิงลึก (In-depth Interview) กับบุคคลผู้ที่เกี่ยวข้องเพื่อรวบรวมข้อมูล ข้อเท็จจริง ปัญหาอุปสรรคที่เกี่ยวข้อง รวมถึงความเห็นและข้อเสนอแนะต่าง ๆ จากผู้ที่เกี่ยวข้อง

๑.๒ ประชากรและกลุ่มตัวอย่าง

๑.๒.๑ เจ้าหน้าที่ตำรวจ

๑.๒.๒ ผู้แทนในคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งค์โทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง ประกอบด้วย ผู้แทนกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ผู้แทนธนาคารแห่งประเทศไทย และผู้ช่วยเลขาธิการ กสทช. ด้านกิจการโทรคมนาคม

๒. การวิเคราะห์ข้อมูล

ในการวิเคราะห์ข้อมูลนั้น ผู้วิจัยใช้วิธีการวิเคราะห์ช่องว่าง (Gap Analysis) เพื่อหาความแตกต่างระหว่างรูปแบบและพฤติกรรมการหลอกลวงกับการดำเนินมาตรการในการแก้ไขและป้องกันปัญหาดังกล่าว เพื่อนำไปสู่การนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

๓. การนำเสนอข้อมูล

นำเสนอข้อมูลและสรุปผลการศึกษาโดยใช้รูปแบบการพรรณนาอธิบายเชื่อมโยงข้อค้นพบเพื่อนำไปสู่การนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทำให้ทราบถึงพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่และผลกระทบที่เกิดขึ้นต่อสังคมและผู้บริโภค

๒. ทำให้ทราบถึงแนวทางการดำเนินการเพื่อแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ในเชิงนโยบาย กฎหมาย เทคโนโลยี และอื่น ๆ ทั้งในประเทศและต่างประเทศ รวมถึงปัญหาและอุปสรรคในการดำเนินการ เพื่อนำไปสู่ข้อเสนอแนะเชิงนโยบายและมาตรการในการเพิ่มประสิทธิภาพในการแก้ไขและป้องกันการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย

๓. สามารถนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ ทั้งในส่วนของหน่วยงานภาครัฐที่เกี่ยวข้อง ผู้ให้บริการโทรศัพท์เคลื่อนที่ ผู้ให้บริการโทรคมนาคมที่เกี่ยวข้อง และผู้บริโภค ซึ่งจะเป็นการลดความเสี่ยงที่จะเกิดความเสียหายจากการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่กับประชาชนและสามารถยกระดับการป้องกันภัยต่อความมั่นคงของประเทศอันเกิดจากการหลอกลวงดังกล่าว

คำจำกัดความ

กิจการโทรคมนาคม หมายถึง กิจการซึ่งให้บริการการส่ง การแพร่ หรือการรับเครื่องหมาย สัญญาณ ตัวหนังสือ ตัวเลข ภาพ เสียง รหัส หรือสิ่งอื่นใด ซึ่งสามารถให้เข้าใจความหมายได้โดยระบบคลื่นความถี่ ระบบสาย ระบบแสง ระบบแม่เหล็กไฟฟ้า หรือระบบอื่น ระบบใดระบบหนึ่งหรือหลายระบบรวมกัน และรวมถึงกิจการซึ่งให้บริการดาวเทียมสื่อสาร หรือกิจการอื่นที่ กสทช. กำหนดให้เป็นกิจการโทรคมนาคม แต่ไม่รวมถึงกิจการที่เป็นกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการวิทยุคมนาคม

สำนักงาน กสทช.	หมายถึง	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) เป็นองค์กรอิสระของรัฐที่จัดตั้งขึ้นตามพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบ กิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. ๒๕๕๓ อันเป็นกฎหมายที่ตราขึ้นให้เป็นไปตามมาตรา ๔๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๕๐ มีหน้าที่สำคัญในการจัดสรรและการกำกับดูแลการใช้คลื่นความถี่ในการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม รวมทั้งกิจการดาวเทียมสื่อสาร ให้เกิดประโยชน์สูงสุดแก่ประชาชน และการพัฒนาประเทศ
Call Center	หมายถึง	ศูนย์รวมหรือผู้ที่มีบทบาทหน้าที่ในการรวมสายเข้าและโทรออกภายในสำนักงาน เพื่อบริหารจัดการการโทรเข้า-ออกจำนวนมากในแต่ละวันให้มีประสิทธิภาพมากขึ้น รวมทั้งยังใช้เป็นช่องทางในการตอบสนองความต้องการของลูกค้าที่ต้องการติดต่อสอบถามข้อมูล ทั้งเรื่องเกี่ยวกับผลิตภัณฑ์ และขอความช่วยเหลือเพื่อแก้ปัญหา
แก็งค์ Call Center	หมายถึง	อาชญากรรมทางเศรษฐกิจรูปแบบหนึ่งในยุคดิจิทัลมีรูปแบบการทำงานเป็นขบวนการ มีการแบ่งหน้าที่ชัดเจนโดยการใช้ช่องทางความตื่นกลัว ความโลภ และการสร้างความสัมพันธ์อันดีกับเหยื่อหรือผู้เสียหาย เพื่อหลอกลวงให้เหยื่อหลงเชื่อและโอนเงินเข้าบัญชีธนาคารของคนร้ายที่ได้เตรียมเปิดรองรับไว้

บทที่ ๒
แนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้อง

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่โดยเฉพาะอย่างยิ่งภัยการหลอกลวงทางโทรศัพท์มิจฉาชีพคอลเซ็นเตอร์ หรือแก๊งคอลเซ็นเตอร์ (Call Center) ถือเป็นภัยทางสังคมระดับชาติและเป็นภัยต่อความมั่นคงของประเทศ เป็นอาชญากรรมทางสังคมที่สำคัญซึ่งส่งผลกระทบกับประชาชนและมั่นคงในวงกว้าง มีประชาชนจำนวนมากถูกหลอกลวงและสูญเสียทรัพย์สิน จึงเป็นปัญหาที่ภาครัฐจะต้องดำเนินการแก้ไข อย่างไรก็ดีเพื่อนำไปสู่ข้อเสนอแนะสำหรับการแก้ไขปัญหาซึ่งเป็นวัตถุประสงค์สำคัญของงานวิจัยนี้ จำเป็นต้องจะต้องมีการศึกษางานวิจัยที่เกี่ยวข้อง รวมทั้งงานศึกษาและกรณีศึกษาในต่างประเทศ เพื่อเป็นแนวทางในการศึกษา และทำให้การวิจัยสามารถดำเนินไปได้อย่างถูกต้อง มีความน่าเชื่อถือ ในบทนี้จึงเป็นการนำเสนอแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องรวมทั้งกรณีศึกษาในต่างประเทศซึ่งมีการนำมาประยุกต์ใช้กับงานวิจัยชิ้นนี้ ได้แก่

๑. ทฤษฎีและแนวคิดที่เกี่ยวข้องกับการหลอกลวงหรือพฤติกรรมของผู้กระทำผิด งานวิจัยชิ้นนี้ได้มีการนำแนวคิดหรือทฤษฎีในการหลอกลวงของมิจฉาชีพประกอบด้วย ๘ หลักการ คือ ๑) หลักการเบี่ยงเบนความสนใจ ๒) หลักการปฏิบัติตามเงื่อนไขในสังคม ๓) หลักการคล้อยตามคนหมู่มาก ๔) หลักการความซื่อสัตย์ ๕) หลักการความใจดี ๖) หลักการความอยากได้อยากมี และความโลภ หรือการตอบสนองต่อความต้องการพื้นฐานของมนุษย์ ๗) หลักการด้านเวลา และ ๘) หลักการสร้างข้อผูกพัน โดยหลักการเหล่านี้ได้ประมวลจากงานศึกษาหลายงาน (Buchanan & Witty, 2012; Button et al., 2014; Cialdini & Goldstein, 2002; Lea et al., 2009; Modic & Lea, 2013; Stejano & Wilson, 2009; 2011)

๒. ทฤษฎีและงานศึกษาที่เกี่ยวข้องกับผู้เสียหาย งานวิจัยชิ้นนี้ได้ใช้ทฤษฎีที่เกี่ยวข้องกับการตัดสินใจของผู้เสียหาย คือ ทฤษฎีข้อผิดพลาดในการตัดสินใจ (Error of Judgement) ของ Lea, Fischer และ Evans (2009) ซึ่งได้อ้างอิงทฤษฎีความคุ้นชินและอคติ (Heuristics and Biases) ของ Tversky และ Kahneman (1974)

๓. ทฤษฎีที่อธิบายทั้งในส่วนของผู้กระทำผิดและผู้เสียหาย นอกจากการใช้ทฤษฎีอธิบายในส่วนที่เกี่ยวข้องกับฝั่งผู้กระทำผิดและผู้เสียหายแล้ว ยังมีการใช้ทฤษฎีที่อธิบายความเชื่อมโยงขององค์ประกอบต่าง ๆ อย่างครบถ้วน คือ ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ของสุมนทิพย์ และคณะ (๒๕๖๓: หน้า ๓๑)

๔. กรณีศึกษาในต่างประเทศ ในงานวิจัยชิ้นนี้ได้มีการนำเสนอกรณีศึกษาต่างประเทศเพื่อเป็นแนวทางในการเปรียบเทียบและประยุกต์ใช้สำหรับข้อเสนอแนะในการแก้ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย โดยได้นำเสนอแนวทางในการแก้ปัญหาดังกล่าวในสหรัฐอเมริกา สหราชอาณาจักร ออสเตรเลีย และสิงคโปร์

รายละเอียดของแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องข้างต้นนั้น จะได้มีการอธิบายในรายละเอียดต่อไป

ความสำคัญของปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

๑. ความเสียหายต่อความอยู่ดีมีสุขของประชาชน

ปัญหาการหลอกหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่โดยเฉพาะอย่างยิ่งภัยการหลอกลวงทางโทรศัพท์ มิจฉาชีพคอลเซ็นเตอร์ หรือแก๊งคอลเซ็นเตอร์ (Call Center) เป็นปัญหาที่กระทบต่อความเป็นอยู่ของประชาชนเป็นอย่างยิ่ง โดยจากข้อมูลในปี ๒๕๖๔ มีผู้เสียหายเข้าแจ้งความกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กว่า ๑,๖๐๐ ราย มูลค่าความเสียหายสูงกว่า ๑,๐๐๐ ล้านบาท เมื่อพิจารณาถึงความเสียหายที่เกิดขึ้นในต่างประเทศ ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์หรือบริการส่งข้อความ (Scam calls and texts) เป็นปัญหาร่วมที่เกิดขึ้นในหลายประเทศทั่วโลก ทั้งประเทศที่พัฒนาแล้วและกำลังพัฒนา ปัญหานี้ทำให้เกิดความเสียหายต่อประชาชนเป็นจำนวนมาก เช่น จากข้อมูลของ The Federal Bureau of Investigation’s Internet Crime Complaint Center ในปี ๒๐๒๑ รายงานว่าปัญหาการหลอกลวงโดยใช้โทรศัพท์และข้อความเป็นปัญหาใหญ่ในสหรัฐอเมริกา ประชาชนจำนวนมากถูกหลอกผ่านช่องทางการสื่อสารต่าง ๆ ทั้งการโทรด้วยเสียง ข้อความสั้น (SMS) และข้อความผ่านสื่อโซเชียลมีเดีย จากข้อมูลการแจ้งความของผู้เสียหาย พบว่าในปีหนึ่ง ๆ มีการสูญเสียทรัพย์สินมูลค่ากว่า ๖.๙ พันล้านดอลลาร์สหรัฐ จากผู้เสียหายที่ได้ร้องเรียนเข้ามากว่า ๘๔๗,๓๗๖ กรณี (FBI, 2021) นอกจากนี้ จากข้อมูลการสำรวจผ่านแอพพลิเคชั่น Truecaller พบว่าร้อยละ ๒๒ ของประชากรผู้ใหญ่จำนวน ๒,๐๐๐ รายในสหรัฐอเมริกาได้ตกเป็นเป้าหมายหรือตกเป็นผู้เสียหายจากการหลอกลวงทางโทรศัพท์ในช่วง ๑๒ เดือนที่ผ่านมา (Bhattacharjee, 2021)

นอกจากนี้ ยังมีรายงานว่าผู้ที่ตกเป็นเป้าหมายของมิจฉาชีพหรือสแกมเมอร์ (Scammers) มีความเสียหายทางสุขภาพจิต ไม่ว่าจะเป็นผู้เสียหายที่ได้เสียทรัพย์สินให้แก่มิจฉาชีพหรือไม่ โดยผู้ที่ได้มีการสูญเสียทรัพย์สินไปให้กับมิจฉาชีพมักจะรู้สึกโทษตัวเองที่เสียรู้ให้กับมิจฉาชีพ จึงไม่กล้าที่จะปรึกษาผู้อื่นด้วยกลัวว่าจะถูกประณามหรือต่อว่า นอกจากนี้ ยังทำให้ปัญหาเหล่านี้แก้ไขได้ยากขึ้น เพราะผู้เสียหายมักไม่เปิดเผยข้อมูลทั้งหมดให้กับเจ้าหน้าที่ และการเก็บปัญหาไว้กับตัวเองก็สามารถนำไปสู่ปัญหาการแยกตัวออกจากสังคม (Isolated) อีกด้วย นอกจากผู้ตกเป็นเหยื่อจะต้องเผชิญปัญหาด้านสุขภาพจิตแล้ว ผู้ที่ตกเป็นเป้าหมายหรือถูกคุกคามจากมิจฉาชีพแม้ยังไม่มีการเสียทรัพย์มักประสบปัญหาวิตกกังวล หวาดระแวง หงุดหงิดรำคาญ (ACMA, 2019; Ofcom, 2022) เป้าหมายจำนวนมากรายงานว่าตนเองเสียเวลา และอาจมีการลบหรือบล็อกสายโทรเข้าหรือข้อความที่สำคัญไป ทำให้ไม่ได้รับข้อความหรือสายโทรเข้าจากเพื่อน ญาติ หรือผู้ที่มีความจำเป็นต้องติดต่อ ซึ่งทำให้เสียสุขภาพจิตและเงิน เช่น พลาดโอกาสในการได้รับข้อเสนอที่ดีที่ทำให้ได้รับประโยชน์จากบริษัทต่าง ๆ นอกจากนี้ ผู้ใช้งานโทรศัพท์จำนวนมากยังจำเป็นต้องเสียเงินเพิ่มเพื่อใช้ระบบป้องกันมิจฉาชีพหรือสายเรียกเข้าที่น่าสงสัยอีกด้วย

๒. ความเสียหายต่อผู้ประกอบการและหน่วยงานที่เกี่ยวข้อง

ในแง่ของผลกระทบเศรษฐกิจ นอกจากเงินที่เสียไปแล้ว ยังมีบริษัทหลายแห่งที่ได้รับผลกำไรน้อยลงเพราะไม่สามารถเข้าถึงลูกค้าได้จากการที่ผู้ใช้บริการเลือกที่จะปิดกั้นสายเรียกเข้าที่ไม่คุ้นเคย บริษัทอีกหลายแห่งต้องใช้บริการป้องกันและจัดการมิจฉาชีพเพื่อดูแลลูกค้าของตน ซึ่งนับเป็นเงินลงทุนที่เสียไปเพิ่มเติม ซึ่งยังรวมถึงหน่วยงานของรัฐ ที่ต้องใช้งบประมาณในการจัดการปัญหาดังกล่าวเพิ่มมากขึ้น

๓. ความเสียหายต่อความมั่นคงของชาติ

เนื่องจากปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เป็นปัญหาที่กระทบต่อการเป็นอยู่ของประชาชนเป็นอย่างยิ่ง ดังที่ได้มีการอธิบายข้างต้น จึงสามารถพิจารณาได้ว่าเป็นปัญหาที่กระทบต่อความมั่นคงของชาติ โดยเฉพาะอย่างยิ่งความมั่นคงที่ได้มีการกำหนดไว้ในยุทธศาสตร์ชาติ (พ.ศ. ๒๕๖๑ – ๒๕๘๐) ยุทธศาสตร์ชาติเป็นการกำหนดขึ้นโดยรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา ๖๕ เพื่อการพัฒนาประเทศอย่างยั่งยืน โดยมีวิสัยทัศน์ “ประเทศมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง” ยุทธศาสตร์ชาติได้ประกอบด้วย ๖ ยุทธศาสตร์ ได้แก่ ๑) ยุทธศาสตร์ชาติด้านความมั่นคง ๒) ยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน ๓) ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ ๔) ยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม ๕) ยุทธศาสตร์ชาติด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรต่อสิ่งแวดล้อม ๖) ยุทธศาสตร์ชาติด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ เมื่อพิจารณายุทธศาสตร์ทั้ง ๖ แล้วนั้น จะเห็นได้ว่าปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เป็นภัยคุกคามที่ก่อให้เกิดความเสียหายต่อความอยู่ดีมีสุขของประชาชน กระทบต่อความปลอดภัยในชีวิตและทรัพย์สิน และยังอาจพิจารณาได้ว่ามีผลกระทบต่อความมั่นคงของชาติอีกด้วย จึงจัดได้ว่าปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นปัญหาที่อยู่ในยุทธศาสตร์ชาติข้อที่ ๑ หรือ ยุทธศาสตร์ชาติด้านความมั่นคง ยุทธศาสตร์ข้อนี้มีเป้าหมายสำคัญในภาพรวมระยะเวลา ๒๐ ปีที่เป็นรูปธรรมชัดเจนคือ “ประเทศชาติมั่นคง ประชาชนมีความสุข” โดยประเด็นสำคัญของยุทธศาสตร์ชาติด้านความมั่นคงนั้นคือ การรักษาความสงบภายในประเทศ ที่มุ่งเน้นเสริมสร้างความสงบเรียบร้อยสันติสุขให้เกิดขึ้นกับประเทศชาติบ้านเมือง รวมทั้งทำให้ประชาชนอยู่ดีมีสุข มีความมั่นคงปลอดภัยทั้งในชีวิตและทรัพย์สิน มีความมุ่งมั่นที่จะแก้ไขปัญหาเดิมที่กระทบต่อความมั่นคง เสริมสร้างความร่วมมือกันระหว่างหน่วยงานหลักและรองในการป้องกัน แก้ไขปัญหา และช่วยเหลือประชาชน ทั้งจากภัยคุกคามและปัญหาที่ส่งผลต่อความมั่นคงต่าง ๆ ตลอดจนติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่

ดังนั้น เมื่อพิจารณาแล้วว่าปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เป็นปัญหาที่ได้กำหนดไว้ในยุทธศาสตร์ด้านความมั่นคงแล้ว จึงเป็นปัญหาที่ต้องได้รับการแก้ไขและเป็นหน้าที่สำคัญของภาครัฐ โดยเฉพาะอย่างยิ่งสำนักงาน กสทช. ที่เป็นหน่วยงานที่ทำหน้าที่กำกับดูแลในกิจการโทรคมนาคม และยังเป็นสาเหตุประการสำคัญของการจัดทำงานวิจัยฉบับนี้เพื่อนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย เพื่อให้มีการแก้ไขปัญหาอย่างเหมาะสมและทำให้บรรลุวัตถุประสงค์ที่ตั้งไว้ในยุทธศาสตร์ชาติ

หลักการ แนวคิด และงานศึกษาที่เกี่ยวข้อง

ด้วยปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เป็นปัญหาที่มีความรุนแรงจึงมีการพิจารณาว่าเป็นปัญหาระดับประเทศในหลายประเทศทั่วโลก และได้มีการศึกษารวมทั้งแนวทางการแก้ปัญหาดังกล่าวจากหลายสาขาวิชาเพื่อทำความเข้าใจลักษณะที่มาของปัญหาทั้งจากผู้กระทำผิดและผู้ตกเป็นเป้าหมาย เช่น จิตวิทยาเพื่อทำความเข้าใจสภาวะการตัดสินใจของเหยื่อ หลักการต่าง ๆ ที่มิจฉาชีพหรือสแกมเมอร์ (Scammers) ใช้ในการล่อลวงเหยื่อหรือเป้าหมาย การสร้างระบบเพื่อปกป้องประชาชนจากมิจฉาชีพและแนวทางการแก้ปัญหาของภาครัฐ

๑. หลักการที่มิจฉาชีพใช้ในการหลอกลวง

หนึ่งในวิธีการแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความที่มักมีการกล่าวถึงบ่อยครั้งคือการให้ความรู้แก่ประชาชน แต่การให้ความรู้อย่างครบถ้วนจำเป็นต้องทำความเข้าใจการทำงานหรือวิธีการของมิจฉาชีพ ซึ่งการทำความเข้าใจมิจฉาชีพยังทำให้สามารถวางมาตรการที่เหมาะสมได้ดียิ่งขึ้น ปัญหาการหลอกลวงทางโทรศัพท์และข้อความรวมทั้งการหลอกลวงผ่านสื่อออนไลน์มักถูกกล่าวถึงในฐานะที่เป็นปัญหาอันเกิดจากการพัฒนาของเทคโนโลยีที่มากขึ้น (Buchanan & Whitty, 2012; Button et al., 2014) ทำให้มิจฉาชีพสามารถใช้ช่องว่างของเทคโนโลยีหลอกลวงประชาชนได้โดยง่ายขึ้น เช่น การโทรออกหรือส่งข้อความได้ในราคาถูกแต่ส่งถึงเป้าหมายเป็นจำนวนมากในเวลาเดียวกันได้ และสามารถเข้าถึงเป้าหมายแม้จะอยู่คนละประเทศ (พัลลภ หริ่งรอด, ๒๕๖๒: หน้า ๗; จักรพงษ์ กังวานโสภณ, ๒๕๖๕: หน้า ๒๘๐) ทว่า งานศึกษาของ Stejano และ Wilson (2009; 2011) พบว่าปัญหาการหลอกลวงเหล่านี้มิได้ขึ้นอยู่กับเทคโนโลยีเป็นส่วนใหญ่ เพราะวิธีการที่มิจฉาชีพนำมาใช้เป็นหลักการดั้งเดิมที่เคยใช้ตั้งแต่ยังไม่มีการคิดค้นคอมพิวเตอร์ และหลักการเหล่านี้เป็นการโจมตีจุดอ่อนของความเป็นมนุษย์ที่ทุกคนมี (Lea et al., 2009) อย่างไรก็ดี งานศึกษาข้างต้นได้อธิบายถึงหลักการที่มิจฉาชีพใช้รวมทั้งจุดอ่อนที่ทำให้ประชาชนจำนวนมากตกเป็นเป้าหมาย ซึ่งหลักการหลายประการมีความคล้ายคลึงกัน นอกจากนี้ หลักการหลายประการได้มีการอธิบายไว้ในจิตวิทยาของการโน้มน้าวจิตใจด้วย (Psychology of Persuasion) (Cialdini & Goldstein, 2002; Modic & Lea, 2013) โดยสามารถสรุปหลักการดังกล่าวได้ดังนี้

๑) หลักการเบี่ยงเบนความสนใจ (Distraction Principle) มิจฉาชีพมักใช้หลักการในการเบี่ยงเบนความสนใจกับเป้าหมาย โดยเมื่อเป้าหมายได้ถูกดึงดูดความสนใจไปที่สิ่งหนึ่งสิ่งใดแล้ว เป้าหมายจะไม่ทันสังเกตความผิดปกติอื่น ๆ ที่เกิดขึ้น หลักการนี้นับได้ว่าเป็นหลักการพื้นฐานของมิจฉาชีพและถูกนำไปใช้ในการล่อลวงต่าง ๆ มากมาย เช่น การหลอกลวงที่ชื่อว่า “419” ในประเทศไนจีเรีย โดยมิจฉาชีพจะหลอกเป้าหมายว่าเป็นเจ้าหน้าที่ของรัฐที่สามารถเข้าถึงเงินหลายสิบล้านดอลลาร์ โดยจะหลอกล่อเป้าหมายให้ช่วยลักลอบนำเงินดังกล่าวออกนอกประเทศ และมีค่าตอบแทนให้จำนวนหนึ่ง และเมื่อเป้าหมายตอบตกลง มิจฉาชีพก็จะให้เป้าหมายโอนเงินจำนวนหนึ่งมาให้ก่อนเมื่อเป็นค่าใช้จ่ายในการดำเนินการและเป้าหมายจะถูกขอให้โอนเงินอีกหลายครั้งโดยให้ความหวังเป้าหมายว่าจะได้รับเงินจำนวนมากเมื่อแผนการโอนเงินข้ามประเทศสำเร็จ หลักการสำคัญของการล่อลวงลักษณะนี้คือการทำให้เป้าหมายมุ่งเป้าความสนใจทั้งหมดไปที่เงินจำนวนมากที่จะได้รับตอบแทน ซึ่งทำให้เป้าหมายมองข้ามความผิดปกติอื่น ๆ และการปกป้องตนเองไปชั่วขณะ

๒) หลักการการปฏิบัติตามเงื่อนไขในสังคม (Social Compliance Principle) หรือหลักการที่คนในสังคมจะยึดถือหรือปฏิบัติตามกฎเกณฑ์ต่าง ๆ ในสังคมร่วมกัน เช่น การที่คนในสังคมถูกหล่อหลอมให้ไม่คิดตั้งคำถามกับการกระทำของรัฐหรือองค์กรที่มีอำนาจในสังคม (Authority) ซึ่งทำให้เกิดการ “ไม่สงสัยในสิ่งที่ควรสงสัย” (Suspension of suspiciousness) นอกจากนี้ การปลอมเป็นเจ้าหน้าที่ของรัฐทำให้มีความน่าเชื่อถือ (Credibility) และทำให้เป้าหมายเกิดความไว้เนื้อเชื่อใจ (Trust) โดยง่าย ซึ่งหลักการนี้ถูกนำไปใช้โดยมิจฉาชีพจำนวนมาก เช่น เจ้าของร้านเครื่องเพชรยอมยกสร้อยคอและเงินสดจำนวนหนึ่งให้มิจฉาชีพที่ปลอมตัวเป็นตำรวจ โดยมิจฉาชีพอ้างว่าจะนำของเหล่านั้นไปใช้เป็นหลักฐานในคดีและจะนำมาคืนภายหลัง เจ้าของร้านยอมทำตามโดยมิได้ตั้งข้อสงสัยและเชื่อใจโดยง่ายเพราะความน่าเชื่อถือของอาชีพตำรวจ นอกจากนี้ หลักการนี้ยังได้มีการอธิบายโดยศาสตร์ของการโน้มน้าวจิตใจว่าคนมักเชื่อบุคคลที่มีตำแหน่งน่าเชื่อถือ แม้ว่าการกระทำหรือคำพูดจะฟังดูไม่มีเหตุผล

๓) หลักการการคล้อยตามคนหมู่มาก (Herd Principle) คือหลักการที่คนมักตัดสินใจทำตามคนหมู่มากโดยไม่ได้สังเกตความผิดปกติ ในบางงานศึกษา ได้เรียกหลักการนี้ว่า “Social Validation” หรือการตัดสินใจตามคนส่วนใหญ่เพราะคิดว่าทางเลือกนั้นได้รับการเห็นชอบจากคนในสังคมแล้ว การใช้หลักการนี้ มิจฉาชีพจะต้องใช้หน้าม้าเข้ามาช่วย ซึ่งเป็นส่วนที่มีผลอย่างมาก เช่น การเสี่ยงประมูลหรือในการพนัน เมื่อผู้คนรอบตัวหรือหน้าม้ากล้าเสี่ยงเลือกตัวเลือกที่ไม่สมเหตุสมผล เป้าหมายจะรู้สึกมั่นใจเพราะไม่ใช่ตัวเองคนเดียวที่อยู่ในความเสี่ยง และเลือกเสี่ยงตามคนหมู่มาก หรือในการประมูลออนไลน์ มักมีการใช้หน้าม้าเข้ามาทำให้ดูเหมือนมีการประมูลกันจริง แม้แต่ในการเลือกตั้งก็ยังมีการใช้หลักการนี้ ซึ่งหลักการนี้ยิ่งได้ผลมากขึ้นในระบบที่ใช้การบอกปากต่อปาก (Peer-to-peer)

๔) หลักการความไม่ซื่อสัตย์ (Dishonesty principle) เป็นหลักการที่มิจฉาชีพจะหลอกล่อเหยื่อให้กระทำความผิดเพื่อให้เป้าหมายไม่กล้าแจ้งความดำเนินคดี แม้เป้าหมายจะรู้ว่ากำลังถูกโกง ด้วยกลัวว่าตนเองจะถูกดำเนินคดีเช่นกัน ตัวอย่างเช่น ในการล่อลวง 419 ในประเทศไนจีเรีย สาเหตุหนึ่งที่เกิดความเสียหายเป็นจำนวนมากเพราะเหยื่อไม่ยอมแจ้งความโดยมิจฉาชีพได้ทำให้ผู้เสียหายตกอยู่ในสถานะที่มีความผิดเช่นกัน จึงไม่สามารถขอความช่วยเหลือจากรัฐได้ เหยื่อของไวรัส Trojan จำนวนมากไม่กล้าแจ้งความเพราะได้รับไวรัสจากการเข้าชมสื่อลามกผิดกฎหมาย ผู้เสียหายจำนวนมากจึงได้รับความเสียหายอย่างรุนแรงจนถึงการล้มละลายไปจนถึงฆ่าตัวตายด้วยความคิดว่าไม่มีทางออก

๕) หลักการความใจดี (Kindness Principle) มิจฉาชีพมักใช้ความใจดีและความยินดีที่จะช่วยเหลือผู้อื่นของเป้าหมายในการหลอกลวง หลักการนี้มีความคล้ายคลึงกับหลักการคนมักทำความดีตอบแทนผู้อื่น (Reciprocation Principle) ของ Cialdini (Cialdini, 2001) การหลอกลวงลักษณะนี้มักมาในรูปแบบการกุศล โดยมักใช้ภาพสื่อที่มีผู้คนนองน้ำตา ประสบภัยพิบัติประกอบการหลอกลวง เช่น ภาพภัยพิบัติสึนามิ แผ่นดินไหว ทำให้คนรู้สึกสงสารและอยากช่วยเหลือ

๖) หลักการความอยากได้อยากมีและความโลภ (Need and Greed Principle) หรือหลักการตอบสนองตามต้องการพื้นฐานของมนุษย์ (Visceral triggers) มนุษย์ทุกคนล้วนแต่มีความต้องการ มีความอยากได้อยากมี รวมทั้งมีความหวาดกลัว และความต้องการเป็นที่

ยอมรับ ซึ่งมิจฉาชีพก็เข้าใจจุดนี้เป็นอย่างดี จากกรณีการล่อลวง 419 พบว่าผู้คนจะสามารถตกเป็นเหยื่อได้ง่ายขึ้นหากมีความต้องการเงินมากกว่าปกติหรือกำลังประสบปัญหาด้านการเงิน เมื่อมีการหยิบยื่นโอกาสมาให้ จึงไม่ได้ตั้งข้อสงสัยอย่างที่ควรจะเป็น เหยื่อบางรายไม่ได้มีนิสัยโลภมากเพียงแต่มีความต้องการเป็นที่ยอมรับ เมื่อมีการโดนหลอกว่าเป็นเจ้าชายจากไนจีเรียส่งอีเมลมาให้จึงพร้อมที่จะเชื่อโดยไม่สงสัย นอกจากนี้ ความต้องการทางเพศยังเป็นอีกสาเหตุที่ทำให้หลักการนี้ประสบความสำเร็จ เช่น การหลอกลวงให้หลงรัก (Romance scams) ได้ใช้ความต้องการทางเพศเป็นตัวผลักดันให้การหลอกลวงประสบผลสำเร็จ

๗) หลักการด้านเวลา (Time Principle) มิจฉาชีพมักใช้หลักการนี้ด้วยเข้าใจดีว่ามนุษย์สามารถตัดสินใจผิดพลาดได้ง่ายหากเวลามีจำกัด มิจฉาชีพจึงต้องบีบให้เป้าหมายเลือกทางเลือกที่ตนต้องการให้ได้ในเวลาที่น้อยที่สุด ซึ่งทำให้เป้าหมายไม่มีเวลาทบทวนเข้าใจสถานการณ์อย่างถี่ถ้วน ซึ่งหลักการนี้ได้มีการอธิบายในอีกชื่อหนึ่งว่า หลักการความจำกัด (Scarcity) ซึ่งโดยส่วนใหญ่หมายถึงความจำกัดของเวลา หลักการนี้แสดงถึงความขัดแย้งกับหลักการทางเศรษฐศาสตร์ว่ามนุษย์มีเหตุผล (Rational) โดยวิธีการนั้น มิจฉาชีพจะล่อเป้าหมายให้ยอมรับเงื่อนไขที่ดีมากอย่างที่ยากจะปฏิเสธในเวลาที่จำกัด ทำให้เป้าหมายมักพลาดตอบตกลงไปโดยไม่ทันได้ทบทวนเงื่อนไขหรือความไม่สมเหตุสมผลของข้อเสนอเหล่านั้น

๘) หลักการสร้างข้อผูกพัน (Commitment) วิธีการที่มิจฉาชีพใช้อีกวิธีหนึ่งคือการสร้างข้อผูกพันกับเป้าหมายทีละเล็กน้อย เช่น การให้เป้าหมายค่อย ๆ โอนเงินให้จากจำนวนน้อยหลายครั้ง และเพิ่มมากขึ้นในเวลาต่อมา ซึ่งเป็นการสร้างข้อผูกพันให้เป้าหมายไม่สามารถหลุดพ้นได้โดยง่าย (Lea et al., 2009) โดยหลักการนี้มีที่มาจากการที่คนมักจะพยายามทำตามข้อผูกพันหรือสัญญาที่ตนมีกับผู้อื่น

จากการพิจารณาวิธีการที่มิจฉาชีพนำมาใช้ข้างต้น จะเห็นได้ว่าหลักการทั้งหมดล้วนแต่ใช้จุดอ่อนของมนุษย์ทั้งสิ้น โดยการใช้เทคโนโลยีนั้นเป็นการเข้ามาช่วยให้มิจฉาชีพเข้าถึงเป้าหมายได้ง่ายขึ้น ยิ่งเทคโนโลยีถูกพัฒนาไปอย่างรวดเร็ว ปัญหาการหลอกลวงผ่านช่องทางการสื่อสารต่าง ๆ ยิ่งทำได้ง่ายขึ้น ปัญหาจึงมีระดับความรุนแรงที่มากขึ้นตามไปด้วย อย่างไรก็ดี เพื่อให้สามารถทำความเข้าใจปัญหาอย่างรอบด้าน จึงมีความจำเป็นต้องเข้าใจพฤติกรรม การตัดสินใจและปัจจัยแวดล้อมของฝั่งเป้าหมายหรือผู้เสียหายด้วยเช่นกัน โดยงานศึกษาที่มุ่งเน้นไปที่การตอบสนองของเป้าหมายหรือผู้เสียหายจะได้กล่าวถึงในหัวข้อถัดไป

๒. การตัดสินใจของเป้าหมายหรือผู้เสียหาย

นอกจากความพยายามทำความเข้าใจวิธีการที่มิจฉาชีพใช้แล้ว งานศึกษาจำนวนมากได้พยายามที่จะทำความเข้าใจระบบความคิดและการตัดสินใจของผู้เสียหายด้วยเช่นกัน โดยใช้ทฤษฎีทางจิตวิทยาเข้ามาอธิบาย เช่น งานศึกษาของ Lea Fischer และ Evans (2009) ที่พบว่าการตอบสนองต่อมิจฉาชีพของเป้าหมายนั้นสามารถอธิบายได้ว่าเป็นข้อผิดพลาดในการตัดสินใจ (Error of Judgement) งานศึกษาดังกล่าวได้อ้างอิงทฤษฎีเดิมจากหนังสือ Heuristics and Biases ของ Tversky และ Kahneman (1974) ซึ่งใช้ในการอธิบายข้อผิดพลาดในการตัดสินใจของมนุษย์ซึ่งโดยปกติแล้วควรจะสมเหตุสมผลตามทฤษฎี Rational choice theory โดยทฤษฎีของ Tversky และ Kahneman อธิบายว่าการตัดสินใจของมนุษย์ไม่ได้คงที่หรือคงความสมเหตุสมผลทุกครั้ง และอาจ

เบี่ยงเบนจากความสมเหตุสมผลได้ด้วยประสบการณ์เดิมที่แต่ละคนมีหรือความคุ้นชินและด้วยอคติ โดยปัจจัยที่เกี่ยวข้องกับประสบการณ์เดิมที่มีและอคติสามารถแบ่งออกได้ ๒ ประเภทคือ ๑) ปัจจัยที่เกี่ยวกับความรู้และการนึกคิด (Cognitive source of error) เช่น ความรู้เดิม ความเชื่อที่ถูกหล่อหลอมโดยสังคม ภาพจำเกี่ยวกับสิ่งต่าง ๆ และ ๒) ปัจจัยที่เกี่ยวกับอารมณ์ความรู้สึกต่าง ๆ (Motivational source of error) เช่น ความชอบหรือความพึงพอใจ และการควบคุมอารมณ์

นอกจากปัจจัยทางด้านจิตวิทยาแล้ว งานศึกษาหลายชิ้นพบว่าลักษณะของเป้าหมายบางประการมีความสัมพันธ์กับการตอบสนองต่อมิจฉาชีพ เช่น การขาดความสามารถในการควบคุมอารมณ์ เมื่อได้รับข้อเสนอของมิจฉาชีพ จึงไม่สามารถต้านทานได้ (Modic & Lea, 2013) ที่น่าสนใจประการหนึ่งคืองานศึกษาพบว่าผู้เสียหายจำนวนมากมีความรู้ความเข้าใจในเรื่องการหลอกลวงเป็นอย่างดีแต่ตกเป็นเหยื่อของมิจฉาชีพได้ง่ายกว่าคนทั่วไป และเป้าหมายที่มีความรู้ความเข้าใจยังมีความพยายามที่จะสนใจและถลำเข้าไปในการหลอกลวงโดยคิดว่าจะสามารถหลบหลีกได้ทัน ในขณะที่กลุ่มตัวอย่างที่ไม่ได้เป็นเหยื่อกลับเพิกเฉยต่อการหลอกลวงตั้งแต่แรก นอกจากนี้ ยังมีเป้าหมายจำนวนมากเห็นว่าการตอบสนองต่อสแกมเมอร์เป็นเหมือนการพนันที่ยากจะชนะได้ (Long-odds gamble) แต่ก็ตัดสินใจลองเพราะสิ่งตอบแทนที่อาจจะได้มีมูลค่าที่สูงมาก (Modic, 2012; Modic & Lea, 2013) แม้ว่ากลุ่มเป้าหมายนี้ทราบดีว่ากำลังเผชิญกับการหลอกลวง นอกจากนี้ยังพบว่าลักษณะทางประชากรและสังคมยังมีผลต่อความยากง่ายในการตกเป็นเหยื่อของการหลอกลวงได้ โดยงานศึกษาของ Coluccia et al. (2020) พบว่าเหยื่อการหลอกลวงให้หลงรัก (Romantic Scams) มักเป็นเพศหญิงวัยกลางคนที่มีความไม่มั่นคงทางอารมณ์ (Neuroticism) และมีแนวโน้มที่จะหมกมุ่นในเรื่องความรัก ความสัมพันธ์ และงานศึกษาของ Kraiwanit และ Srijaem (2021) ซึ่งได้ศึกษาปัจจัยที่ส่งผลต่อการปลอมแปลงธุรกรรมทางการเงินออนไลน์ โดยพบปัจจัยที่เกี่ยวข้องกับคุณลักษณะของประชากรว่ามีผลต่อการตกเป็นเป้าหมายได้ง่ายขึ้นด้วย ได้แก่ อายุ โดยพบว่าอายุของกลุ่มตัวอย่างที่มากกว่า ๒๐ มีแนวโน้มที่จะสูญเสียเงินน้อยกว่าตัวอย่างที่อายุต่ำกว่า โดยเฉพาะกลุ่มตัวอย่างที่อายุน้อยกว่า ๒๐ ปี โดยผู้ทำการศึกษาวิเคราะห์ว่าอายุที่มากขึ้นอาจทำให้สามารถตัดสินใจได้อย่างสมเหตุสมผลมากกว่า หรืออาจเป็นเพราะกลุ่มตัวอย่างที่มีอายุมากกว่าใช้เวลาบนอินเทอร์เน็ตน้อยกว่า จึงมีความเสี่ยงที่จะตกเป็นเป้าหายได้น้อยกว่า ทั้งนี้ ผลการศึกษานี้อาจมีความแน่นอนได้ เนื่องจากยังมีงานศึกษาอื่น ๆ ที่พบว่าอายุไม่มีผลต่อการตกเป็นเป้าหมาย (Choi et al., 2016)

๓. การศึกษาจากทั้งมุมผู้กระทำผิดและผู้เสียหาย

นอกจากงานศึกษาที่มุ่งเน้นไปที่การศึกษาจากฝั่งผู้กระทำผิดและฝั่งผู้เสียหายแล้ว ยังมีงานศึกษาและทฤษฎีที่อธิบายความเชื่อมโยงของทั้งสองส่วนเข้าด้วยกัน โดยหนึ่งในทฤษฎีที่สำคัญคือทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ซึ่งเป็นทฤษฎีที่อธิบายถึงสาเหตุหรือองค์ประกอบของการเกิดอาชญากรรม โดยแบ่งองค์ประกอบของการเกิดอาชญากรรมได้เป็น ๓ ส่วน หรือเปรียบเป็นสามเหลี่ยม ๓ ด้าน ดังนี้ (สุมนทิพย์ และคณะ, ๒๕๖๓: หน้า ๓๑)

๑) ผู้กระทำผิด หรือมิจฉาชีพ (Criminals) หมายถึง ผู้ที่มีความต้องการที่จะกระทำผิด

๒) เหยื่อ หรือ เป้าหมาย (Victims/Target) หมายถึง บุคคลที่ผู้กระทำผิดหรือมิจฉาชีพมุ่งหมายกระทำผิด

๓) โอกาส (Opportunity) หมายถึง เวลาและสถานที่ที่เหมาะสมให้ผู้กระทำผิดสามารถกระทำผิดได้สำเร็จ

เมื่อพิจารณาจากองค์ประกอบด้านต้น งานศึกษาโดยมากมักมุ่งเน้นไปที่องค์ประกอบที่เป็นตัวบุคคล แต่ยังไม่มีการมุ่งเน้นไปที่องค์ประกอบด้านโอกาส อย่างไรก็ดี ในการป้องกันและแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์ จำเป็นต้องมีการคำนึงถึงองค์ประกอบ ๓ ด้าน ของทฤษฎีสามเหลี่ยมอาชญากรรมโดยจะต้องมีการแก้ไขและวางมาตรการให้เหมาะสมครบทั้ง ๓ ด้าน

๔. ข้อวิเคราะห์และสรุปงานทบทวนงานศึกษาที่เกี่ยวข้อง

จากการทบทวนวรรณกรรมในส่วนที่เกี่ยวข้องกับจิตวิทยาทั้งในส่วนของมิจฉาชีพหรือผู้กระทำความผิดและในส่วนของผู้เสียหาย สามารถกล่าวได้ว่าการหลอกลวงของผู้กระทำผิดมุ่งเน้นไปที่จุดอ่อนของมนุษย์เป็นหลัก ทั้งการใช้ความต้องการพื้นฐานที่มนุษย์ทุกคนมี ข้อกำจัดในกระบวนการตัดสินใจ การสร้างเงื่อนไขหรือสถานการณ์ที่บีบบังคับให้เป้าหมายตกเป็นเหยื่อได้โดยง่าย อย่างไรก็ดี ไม่สามารถปฏิเสธได้ว่าเทคโนโลยีที่พัฒนาอย่างรวดเร็วในปัจจุบันมีผลต่อการขยายตัวของปัญหาเป็นอย่างมาก โดยเทคโนโลยีได้ช่วยให้ผู้กระทำผิดสามารถเข้าถึงเป้าหมายได้มากขึ้น ดังที่เห็นได้จากตัวอย่างการหลอกลวงต่าง ๆ ที่ต้องมีการพึ่งพาเทคโนโลยีการสื่อสารเพื่อเข้าถึงเป้าหมาย ซึ่งการประสานกันทั้งวิธีการทางจิตวิทยาและการใช้เทคโนโลยีทำให้ปัญหาการหลอกลวงมีความรุนแรงมากขึ้น สำหรับกรณีของประเทศไทยที่มีการใช้การโทรข้ามประเทศจากประเทศเพื่อนบ้านซึ่งเป็นการใช้เทคโนโลยีเช่นเดียวกัน เมื่อพิจารณาถึงปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์ที่เกิดขึ้น พบว่าลักษณะการหลอกลวงที่เกิดขึ้นเป็นวิธีการที่ตรงกับการอธิบายของงานศึกษาทางจิตวิทยาต่าง ๆ หลายประการ โดยเฉพาะหลักการการปฏิบัติตามเงื่อนไขในสังคม (Social Compliance Principle) หรือหลักการที่เกี่ยวข้องกับความเชื่อถือในหน่วยงานของรัฐ (Authority) ด้วยลักษณะการหลอกลวงนั้นมักเป็นการหลอกเป้าหมายว่าเป็นเจ้าหน้าที่ของรัฐหรือหน่วยงานที่น่าเชื่อถือ เช่น สำนักงาน กสทช. ตำรวจ หรือธนาคาร ซึ่งการแอบอ้างลักษณะนี้ทำให้เป้าหมายเชื่อฟังคำสั่งของมิจฉาชีพโดยง่าย นอกจากหลักการเรื่องความน่าเชื่อถือของหน่วยงานรัฐแล้ว มิจฉาชีพยังมีการใช้หลักการตอบสนองต่อความต้องการพื้นฐานของมนุษย์ (Visceral triggers) โดยเป็นการกระตุ้นความรู้สึกหวาดกลัวของเป้าหมาย การหลอกลวงในประเทศไทยมักใช้อุบายหลอกให้เป้าหมายกลัวการดำเนินคดี โดยอ้างว่าเป้าหมายมีการกระทำความผิด ซึ่งเป็นประเด็นที่น่าสนใจประการหนึ่งสำหรับกรณีของประเทศไทยคือการที่มิจฉาชีพแอบอ้างว่าตนเองเป็นเจ้าหน้าที่ของรัฐและสามารถทำให้เป้าหมายเชื่อว่าตนเองจะมีความผิดได้ แม้ว่าเป้าหมายจะทราบดีว่าตนเองมิได้กระทำผิด จึงเป็นประเด็นที่อาจมีการศึกษาเพิ่มเติมต่อไปถึงความเชื่อมั่นในเจ้าหน้าที่รัฐของคนไทย และอีกหลักการหนึ่งคือหลักการด้านเวลา (Time Principle) โดยมิจฉาชีพมักบีบบังคับให้เป้าหมายต้องทำการโอนเงินไปให้มิจฉาชีพในเวลาที่กำหนดเท่านั้น ด้วยหลักการหลายข้อประกอบกันนี้ ทำให้คนไทยจำนวนมากตกเป็นผู้เสียหายจากการหลอกลวงทางโทรศัพท์ อย่างไรก็ดี การวิเคราะห์เชิงลึกในประเด็นนี้จะได้มีการนำเสนอต่อไปในส่วนผลการวิจัยของงานศึกษาฉบับนี้

ประเด็นที่สำคัญอีกประการหนึ่งที่ได้รับจากการศึกษาวรรณกรรมที่เกี่ยวข้องด้านจิตวิทยา คือ เป้าหมายหรือเหยื่อมิได้โง่ตามที่สังคมเข้าใจ เนื่องจากการหลอกลวงมิได้โจมตีเป้าหมายที่ความฉลาดหรือความด้อยปัญญา หากแต่มุ่งเน้นไปที่การโจมตีในเรื่องของจิตใจและอารมณ์ความรู้สึก

เป็นหลัก นอกจากนี้ การถูกหลอกยังเป็นปรากฏการณ์ที่สามารถเกิดขึ้นได้ในระบบการตัดสินใจของมนุษย์ปกติ ดังนั้น การตีตราผู้ตกเป็นเป้าหมายหรือเหยื่อว่าโง่ที่เพลี่ยงพล้ำถูกหลอกได้นั้นนอกจากเป็นการลดทอนคุณค่าของเป้าหมายหรือเหยื่อแล้ว ยังทำให้ปัญหาหลอกลวงแก้ไขได้ยากขึ้นด้วย ดังที่เห็นได้จากการที่ผู้เสียหายจำนวนมากเลือกที่จะไม่แจ้งความด้วยความอับอาย หรือให้ข้อมูลแก่เจ้าหน้าที่ไม่ครบ ทำให้ไม่สามารถจับกุมผู้กระทำผิดได้ หน่วยงานที่เกี่ยวข้องที่เข้ามาทำหน้าที่แก้ปัญหาการหลอกลวงจึงต้องตระหนักในประเด็นนี้และอาจพิจารณาถึงการการรณรงค์ในประเด็นดังกล่าวเพื่อให้ประชาชนเข้าใจมากขึ้น ซึ่งสามารถนำไปสู่การให้ความร่วมมือมากขึ้นจากฝ่ายเป้าหมายหรือเหยื่อด้วย

นอกจากนี้ยังมีข้อสังเกตเพิ่มเติมอีกว่าการเพิ่มความตระหนักรู้ให้แก่ประชาชนเพียงอย่างเดียวไม่เพียงพอต่อการแก้ปัญหาการหลอกลวงได้ แม้ว่าจะเป็นส่วนที่สำคัญก็ตาม เพราะจากงานศึกษาหลายชิ้นพบว่าในหลายกรณี ปัจจัยด้านความรู้ความเข้าใจต่อปัญหาการหลอกลวงมิได้ช่วยให้โอกาสในการถูกหลอกลวงลดลงได้ ดังนั้น เมื่อจำเป็นต้องมีการแก้ไขปัญหา หน่วยงานที่เกี่ยวข้องต้องตระหนักว่าการแก้ปัญหาจากทางผู้ตกเป็นเหยื่อหรือเป้าหมายอย่างเดียวนั้นไม่สามารถแก้ปัญหาได้ทั้งหมด แม้ว่าจะมีการพยายามสร้างความตระหนักรู้ในประชาชนแล้ว การมีระบบป้องกันประชาชนจากการถูกหลอกลวงโดยเฉพาะอย่างยิ่งจากหน่วยงานของรัฐจึงเป็นสิ่งจำเป็นในแก้การแก้ปัญหา และการแก้ปัญหาอย่างครบถ้วนจากถูกฝ่ายจะช่วยให้ปัญหาได้รับการแก้ไขได้ดีขึ้น โดยบทบาทและแนวทางของหน่วยงานของรัฐในต่างประเทศจะได้มีการนำเสนอต่อไป

แนวทางการแก้ปัญหาของหน่วยงานที่เกี่ยวข้องในต่างประเทศ

เนื่องจากปัญหาการหลอกลวงทางโทรศัพท์และข้อความเป็นปัญหาที่มีความรุนแรง และมีผลกระทบต่อทั้งประชาชนและเศรษฐกิจเป็นอย่างมาก นอกจากนี้ ด้วยปัญหาที่ไม่สามารถแก้ไขที่ตัวประชาชนเพียงอย่างเดียวได้ หน่วยงานของรัฐในหลายประเทศจึงต้องมีแนวทางในการแก้ไขปัญหาทั้งการป้องกันปัญหาและเยียวยาผู้เสียหาย โดยตัวอย่างประเทศที่หน่วยงานของรัฐมีแนวทางในการแก้ไขปัญหาอย่างจริงจัง มีดังนี้

๑. สหรัฐอเมริกา

สหรัฐอเมริกาเป็นประเทศที่นับได้ว่าประสบปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์และข้อความมากที่สุดประเทศหนึ่ง จากรายงานของ Federal Communications Commission (FCC) พบว่าประชาชนได้รับสายจากการโทรแบบระบบอัตโนมัติที่เรียกว่า Robocall ซึ่งมีเจตนาหลอกลวงให้เสียทรัพย์กว่า ๔ พันล้านครั้งต่อเดือน (FCC, 2022) ด้วยเทคโนโลยีที่พัฒนามากขึ้นในปัจจุบัน ทำให้การโทรในลักษณะดังกล่าวมีต้นทุนที่ต่ำและสามารถโทรไปยังปลายสายได้จำนวนมากในเวลาเดียวกัน นอกจากนี้ เทคโนโลยีที่พัฒนามากขึ้นยังทำให้มิจฉาชีพสามารถปลอมแปลงเลขหมาย (Spoof caller ID) ได้โดยง่าย หน่วยงานภาครัฐของสหรัฐอเมริกาจึงมีความแข็งขันที่จะแก้ปัญหาดังกล่าว ทั้งจากหน่วยงานกำกับดูแลด้านโทรคมนาคมและหน่วยงานอื่น ๆ ที่เกี่ยวข้องดังนี้

๑.๑ แนวทางการแก้ปัญหาหลอกลวงทางโทรศัพท์และข้อความของหน่วยงานกำกับดูแลในกิจการโทรคมนาคม

หน่วยงาน FCC ในฐานะหน่วยงานกำกับดูแลในกิจการโทรคมนาคมได้มีความพยายามแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้น เนื่องจากมิจฉาชีพมักใช้ช่องทางการสื่อสารผ่านทั้งโทรศัพท์ และช่องทางออนไลน์ต่าง ๆ ในการเข้าถึงเป้าหมาย FCC จึงเป็นอีกหน่วยงานหลักในการแก้ไขปัญหาการหลอกลวงดังกล่าว โดยเฉพาะปัญหาที่มาจากระบบการโทรอัตโนมัติ หรือ “Robocall” FCC จึงได้มีการจัดตั้งโครงการ Robocall Response Team ขึ้นในปี ๒๐๑๙ ซึ่งเป็นการร่วมมือกันระหว่างหน่วยงานต่าง ๆ ทั้งภาครัฐ นักกฎหมาย ผู้กำหนดนโยบาย วิศวกร นักเศรษฐศาสตร์ และผู้เชี่ยวชาญด้านต่าง ๆ เพื่อร่วมกันแก้ปัญหาดังกล่าวอย่างจริงจัง โดยนอกจากการสร้างความตระหนักรู้ให้กับประชาชนแล้ว ยังต้องกำหนดมาตรการต่าง ๆ เพื่อร่วมแก้ปัญหานี้ให้มีประสิทธิภาพด้วย ซึ่งมีรายละเอียดดังนี้ (FCC, 2022)

๑) การออกคำสั่งให้ยับยั้งการกระทำผิด (Cease-and-Desist) ไปยังผู้ให้บริการโทรศัพท์ที่มีพฤติการณ์เกี่ยวข้องกับการใช้ Robocall อย่างผิดกฎหมายโดยทันที FCC ได้มีการเฝ้าระวังปัญหาดังกล่าวอย่างใกล้ชิดและดำเนินการโดยทันทีเมื่อพบเห็นการกระทำผิด โดย FCC’s Enforcement Bureau หรือส่วนงานการบังคับใช้กฎหมายของ FCC จะมีคำสั่งยับยั้งการกระทำผิดในลักษณะดังกล่าวไปยังผู้ให้บริการโทรศัพท์ และที่ผ่านมา ได้มีการออกคำสั่งดังกล่าวเป็นจำนวนมาก ซึ่งหากผู้ให้บริการโทรศัพท์ไม่ดำเนินการยับยั้งการกระทำผิดโดยทันที จะมีมาตรการให้ผู้ให้บริการรายอื่นระงับทราฟฟิกที่มาจากผู้ให้บริการรายดังกล่าว

๒) การปรับด้วยจำนวนเงินที่สูง (Major Fines) ที่ผ่านมา FCC ได้มีการปรับเงินผู้กระทำผิดทั้งการใช้การโฆษณาผ่านโทรศัพท์เพื่อหลอกลวงประชน รวมทั้งการปลอมแปลงเลขหมายและใช้ Robocall จากการดำเนินการที่ผ่านมา FCC ได้มีการปรับเงินเป็นจำนวนมากที่สุดถึง ๒๕๕ ล้านดอลลาร์สหรัฐ นอกจากนี้ FCC ได้มีการทำงานอย่างใกล้ชิดกับกระทรวงยุติธรรม (Justice Department) เพื่อดำเนินการฟ้องร้องและคิดค่าเสียหายต่าง ๆ อีกด้วย

๓) การกำหนดให้มีการยืนยันตัวตนของเลขหมายผ่านระบบ STIR/SHAKEN[๑] (Caller ID Authentication (STIR/SHAKEN)) FCC ได้มีการสนับสนุนให้ใช้ระบบ STIR/SHAKEN มาใช้ในการตรวจสอบตัวตนของผู้ใช้เลขหมายระหว่างผู้ให้บริการโทรศัพท์ และทำให้สามารถระงับการใช้งานของเลขหมายที่ปลอมแปลงได้ FCC ได้ยืนยันเมื่อวันที่ ๓๐ มิถุนายน ๒๐๒๑ ว่าผู้ให้บริการโทรศัพท์รายใหญ่ในสหรัฐอเมริกาต่างก็ได้ดำเนินการนำระบบนี้มาใช้ใน IP Sections ในเครือข่ายของตนแล้ว ซึ่งเป็นไปตามที่ FCC กำหนด

---

[๑] STIR/SHAKEN หรือ Secure Telephony Identity Revisited (STIR) และ Secure Handling of Asserted Information Using Tokens (SHAKEN) คือ ระบบการตรวจสอบตัวตนของผู้โทร (Caller ID) โดย STIR จะทำหน้าที่สร้าง Digital Signatures หรือ Digital Certificates สำหรับสายเรียกเข้าผ่านระบบ VoIP ซึ่งเป็นข้อมูลที่ระบุตัวตนของผู้โทร ต้นทาง (Call origin) และข้อมูลผู้ให้บริการ และ SHAKEN ทำหน้าที่กำหนดการใช้ข้อมูลที่ได้จาก STIR ในเครือข่ายของผู้ให้บริการ

๔) การสร้างฐานข้อมูลการดำเนินการแก้ปัญหา Robocall (Robocall Mitigation Database) FCC ได้ขอให้ผู้ให้บริการนำส่งใบรับรองที่ได้จากผู้ให้บริการระบบ STIR/SHAKEN เพื่อรายงานสถานะการดำเนินการ และเพื่อแสดงแนวทางในการแก้ปัญหา Robocall โดยปัจจุบัน ผู้ให้บริการโทรศัพท์หลายรายได้นำส่งใบรับรองที่ยืนยันการใช้ระบบ STIR/SHAKEN อย่างเต็มรูปแบบ ซึ่ง FCC ได้มีการกำหนดเพิ่มเติมว่าหากไม่สามารถนำส่งใบรับรองการใช้ระบบ STIR/SHAKEN อย่างเต็มรูปแบบได้ จะต้องนำเสนอรายละเอียดขั้นตอนการแก้ปัญหาให้กับ FCC แทน เพื่อยืนยันว่าตนมิได้เป็นผู้สนับสนุนการใช้ Robocall ผิดกฎหมาย โดย FCC ได้กำหนดให้เริ่มมีการลงโทษผู้ให้บริการที่ไม่ให้ความร่วมมือโดยกำหนดให้ผู้ให้บริการโทรศัพท์รายอื่นจะต้องปิดกั้นทราฟฟิกจากผู้ให้บริการที่ไม่ได้ใช้ระบบ STIR/SHAKEN และมิได้แสดงรายละเอียดแนวทางแก้ปัญหา Robocall หลังเดือนกันยายน ๒๐๒๑ และตั้งแต่เดือนตุลาคม ๒๐๒๒ ผู้ให้บริการที่ยังไม่ดำเนินการจะถูกถอดออกจากฐานข้อมูล Robocall Mitigation ซึ่งทำให้ทราฟฟิกจากผู้ให้บริการรายนั้นจะถูกปิดกั้นโดยสิ้นเชิงจากผู้ให้บริการรายอื่น ๆ

๕) การปิดเกตเวย์เพื่อป้องกัน Robocall จากต่างประเทศ FCC ได้ออกกฎใหม่เมื่อเดือนพฤษภาคม ๒๐๒๒ ให้สายโทรเข้าจากต่างประเทศจะต้องมาจากเครือข่ายที่เป็นไปตามมาตรฐานของระบบ STIR/SHAKEN และยังให้ผู้ให้บริการเกตเวย์เข้าร่วมในฐานข้อมูล Robocall Mitigation ด้วย โดยจะต้องมีหน้าที่ระงับสายเรียกเข้าที่น่าสงสัย FCC ยังได้มีการร่วมมือกับหน่วยงานในต่างประเทศเพื่อแก้ปัญหา Robocall ร่วมกัน โดยปัจจุบันได้มีความร่วมมือกับออสเตรเลีย บราซิล แคนาดา โรมาเนีย และสหภาพยุโรป นอกจากนี้ FCC ยังได้มีการจัดทำ “Do Not Originate list” หรือการรวบรวมเลขหมายที่ได้มีการใช้งานโดยมิจฉาชีพจากต่างประเทศอีกด้วย

๖) การสร้างกรอบความร่วมมือกับหน่วยงานต่าง ๆ FCC ได้มีความร่วมมือกับหน่วยงานต่าง ๆ มากมาย ทั้ง ๖ สำนักของ FCC เอง เพื่อร่วมกันบังคับใช้กฎหมายเอาผิดกับ Robocall กำหนดนโยบายใหม่ ให้ความรู้ความเข้าใจกับผู้ให้บริการโทรศัพท์ และยังมีความร่วมมือกับหน่วยงานภายนอกอย่าง Federal Trade Commission (FTC) Department of Justice (DoJ) State Attorneys General และยังมีความร่วมมือกับหน่วยงานในต่างประเทศ นอกจากนี้ FCC อยู่ระหว่างการศึกษา TRACED Act (Telephone Robocall Abuse Criminal Enforcement Deterrence) หรือกฎหมายที่จะนำมาใช้ในการปราบปรามมิจฉาชีพอย่างจริงจังด้วย

๗) การสร้างแนวทางการรับมือกับการส่งข้อความอัตโนมัติ (Robotexts) ไปยังผู้ใช้บริการ FCC ได้กำหนดกฎเกณฑ์ในการส่งข้อความไปยังผู้บริโภค โดยการส่งข้อความจะกระทำได้ต่อเมื่อได้มีการยินยอมจากผู้ใช้บริการไว้ล่วงหน้า หรือเป็นการส่งข้อความที่เป็นเหตุฉุกเฉินเท่านั้น โดยการส่งข้อความที่เกี่ยวข้องกับการค้า จะต้องได้รับการยินยอมเป็นลายลักษณ์อักษร ในกรณีที่เป็นข้อความที่ไม่เกี่ยวข้องกับการค้า เช่น ข้อความจากหน่วยงานที่เกี่ยวข้องกับการจัดเก็บภาษี หน่วยงานที่ไม่แสวงหาผลกำไร หน่วยงานที่เกี่ยวข้องกับกิจกรรมทางการเมือง ผู้ใช้บริการสามารถให้การยินยอมด้วยปากเปล่าได้ หากมีการฝ่าฝืน ผู้ส่งจะถูกระงับการใช้งาน

๑.๒ แนวทางการแก้ปัญหาหลอกลวงทางโทรศัพท์และข้อความของหน่วยงานอื่น ๆ

นอกจาก FCC ที่เป็นหน่วยงานกำกับดูแลในกิจการโทรคมนาคมแล้ว ยังมีหน่วยงานอื่น ๆ ที่เกี่ยวข้องเข้ามาร่วมแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นด้วย โดยหน่วยงานที่มีความแข็งขันในการแก้ปัญหาคือ FTC โดยทั่วไปแล้ว FTC เป็นหน่วยงานกำกับดูแลด้านการแข่งขันทางค้า แต่หน้าที่อีกประการที่สำคัญคือการคุ้มครองผู้บริโภค FTC จึงมีแนวทางในการป้องกันและกำจัดปัญหาการหลอกลวงทางการค้า รวมทั้งปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นด้วย โดยหนึ่งในแนวทางที่ FTC ได้กำหนดขึ้นเพื่อแก้ไขปัญหาสแกมคือการจัดทำฐานข้อมูลสแกมต่าง ๆ ในชื่อ “Do Not Call list” ตั้งแต่ปี ๒๐๐๓ เมื่อผู้ได้รับการติดต่อจากมิจฉาชีพก็จะมีการรายงานเข้ามาที่ FTC หลังจากนั้น FTC ก็จะใช้ฐานข้อมูลดังกล่าวร่วมกับหน่วยงานอื่น ๆ เพื่อป้องกันประชาชนจากมิจฉาชีพ ผู้ที่ได้รับการติดต่อจากมิจฉาชีพสามารถส่งต่อสายโทรเข้าที่นั้นไปที่หมายเลข ๗๗๒๖ หรือร้องเรียนผ่านเว็บไซต์ของ FTC เพื่อให้เลขหมายนั้นอยู่ในรายการ Do Not Call list และหน่วยงานที่เกี่ยวข้องจะดำเนินการระงับเลขหมายนั้นต่อไป (FTC, 2022; FTC, n.d.)

อีกหน่วยงานหนึ่งที่มีแนวทางในการคุ้มครองผู้บริโภคจากมิจฉาชีพคือ Consumer Financial Protection Bureau (CFPB) CFPB เป็นหน่วยงานคุ้มครองผู้บริโภคในกิจการด้านการเงิน โดย CFPB จะควบคุมและกำหนดนโยบายในการป้องกันมิจฉาชีพให้แก่สถาบันทางการเงินต่าง ๆ ในสหรัฐอเมริกา และได้มีช่องทางให้ประชาชนที่ได้รับความเสียหายจากมิจฉาชีพในรูปแบบการหลอกลวงที่เกี่ยวข้องกับสถาบันทางการเงินร้องเรียน เพื่อเข้าช่วยเหลือผู้ได้รับความเสียหายหรือส่งต่อให้กับหน่วยงานที่เกี่ยวข้อง (Bloomberg, 2022; CFPB, 2022)

๒. สหราชอาณาจักร

สหราชอาณาจักรเป็นอีกประเทศหนึ่งที่กำลังประสบปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์และข้อความเป็นจำนวนมาก โดยเฉพาะอย่างยิ่งในช่วงการแพร่ระบาดของโรคโควิด-๑๙ (Covid-19) เช่น การส่งข้อความหลอกลวงในการจองคิวฉีดวัคซีนหรือปลอมเป็นพนักงานขนส่งสินค้า ซึ่งการกระทำผิดมาทั้งจากผู้กระทำผิดในประเทศและมาจากต่างประเทศ ในช่วงเวลาสามเดือนพบว่าประชาชนกว่าล้านคนเคยได้รับสายหรือรับข้อความจากมิจฉาชีพ (Ofcom, 2022) หน่วยงานต่าง ๆ ในสหราชอาณาจักรต่างก็มีแนวทางในการแก้ปัญหาดังกล่าว ทั้งหน่วยงานกำกับดูแลในกิจการโทรคมนาคมและหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยมีรายละเอียดดังนี้

๒.๑ แนวทางการแก้ปัญหาหลอกลวงทางโทรศัพท์และข้อความของหน่วยงานกำกับดูแลในกิจการโทรคมนาคม

Office of Communications (Ofcom) ในฐานะหน่วยงานกำกับดูแลด้านกิจการโทรคมนาคมได้มีแนวทางในการแก้ปัญหาซึ่งแบ่งออกได้เป็น ๓ ส่วน ดังนี้ (Ofcom, 2022)

๑) สร้างระบบที่ทำให้สแกมเมอร์เข้าถึงประชาชนได้ยากขึ้น Ofcom ได้สร้างระบบทั้งด้านกฎหมายและทางเทคนิคเพื่อขัดขวางมิจฉาชีพมิให้เข้าถึงประชาชนได้โดยง่าย Ofcom ได้ผลักดันกฎหมายที่บังคับใช้กับผู้ประกอบการเมื่อวันที่ ๑๕ พฤศจิกายน ๒๐๒๒ โดยได้มีการแก้ไข General Condition (GC) C6 ซึ่งเป็นข้อกฎหมายในกฎหมายกำกับดูแลด้านโทรคมนาคมที่ชื่อว่า The Communications Act 2003 ให้มีการกำหนดให้ผู้ประกอบการใช้ระบบข้อมูล Calling

Line Identification (CLI) และจะมีผลบังคับใช้ประมาณพฤษภาคม ๒๐๒๓ ข้อมูล CLI คือการระบุตัวตนของผู้โทรโดยมีการแบ่งปันข้อมูลนี้ระหว่างผู้ให้บริการโทรศัพท์เมื่อมีการโทรออกและ รับสาย Ofcom กำหนดให้ผู้ให้บริการโทรศัพท์จะต้องมีการใช้ CLI (Preiskel & Co, 2022)

ในขณะเดียวกัน Ofcom เข้าไปดูแลการจัดสรรเลขหมายและย้ายเลขหมายของแต่ละผู้ให้บริการด้วย โดยใช้อำนาจทางกฎหมายคือ The General Condition B1 ใน The Communications Act 2003 ซึ่งกำหนดหน้าที่ของผู้ให้บริการที่จะต้องบริหารจัดการเลขหมายให้มีประสิทธิภาพ Ofcom มีการจัดทำขั้นตอนเพื่อป้องกันมิให้เลขหมายหลุดไปถึงมิจฉาชีพได้ และจัดการเลขหมายของหน่วยงานที่ไม่ได้ใช้แล้ว รวมทั้งเลขหมายที่สงวนไว้เพื่อรับสายเท่านั้น เช่น เลขหมายของธนาคารที่ใช้สำหรับให้ผู้ใช้บริการรายงานปัญหาไปที่ธนาคารเท่านั้น ซึ่งหากมีการโทรออกก็อาจคาดการณ์ได้ว่ามิจฉาชีพนำไปใช้

๒) การใช้ความร่วมมือกับหน่วยงานที่เกี่ยวข้อง Ofcom ได้มีความร่วมมือกับหน่วยงานต่าง ๆ ทั้งหน่วยงานทั้งฝ่ายรัฐบาล หน่วยงานกำกับดูแล หน่วยงานที่ทำหน้าที่บังคับใช้กฎหมาย กลุ่มผู้บริโภคต่าง ๆ ภาคเอกชนและอุตสาหกรรมที่เกี่ยวข้อง โดยความร่วมมือโดยมากเป็นการแบ่งปันข้อมูลระหว่างหน่วยงาน ตัวอย่างเช่น ในปี ๒๐๑๘ Ofcom ได้สนับสนุนการจัดตั้งความร่วมมือ “SMS PhishGuard” ซึ่งเป็นความร่วมมือของผู้ให้บริการโทรศัพท์เคลื่อนที่ในสหราชอาณาจักรหรือ Mobile UK ซึ่งประกอบด้วย EE, O2, Vodafone และ Three โดยร่วมมือกับ Mobile Ecosystem Forum (MEF) ซึ่งเป็นองค์กรความร่วมมือด้านผลกระทบต่าง ๆ ต่อระบบนิเวศของโทรศัพท์เคลื่อนที่ (Mobile UK, 2018) ความร่วมมือดังกล่าวจัดตั้งขึ้นเพื่อปกป้องข้อมูลที่ระบุตัวตนของผู้ส่งข้อความ (Sender IDs) โดยให้หน่วยงานที่มีความประสงค์จะส่งข้อความไปยังประชาชน เช่น หน่วยงานภาครัฐ ธนาคาร ดำเนินการลงทะเบียนก่อนส่งข้อความถึงประชาชน โดยเป็นการลดโอกาสที่สแกมเมอร์จะใช้เลขหมายของหน่วยงานเหล่านี้ปลอมแปลงและส่งข้อความหาประชาชน จากรายงานของ MEF ปี ๒๐๒๑ รายงานว่ามีธนาคารและหน่วยงานของรัฐกว่า ๗๐ แห่งลงทะเบียน และมีผู้ส่งกว่า ๑,๕๐๐ รายที่ถูกบล็อก และกว่า ๓๐๐ รายเป็นหน่วยงานรัฐที่ทำหน้าที่เกี่ยวกับการจัดการเรื่องไวรัสโคโรน่า

Ofcom ยังมีความร่วมมือกับหน่วยงานอื่น ๆ ที่อยู่นอกกิจการโทรคมนาคมด้วย เช่น ความร่วมมือกับ UK Finance หรือสถาบันทางการเงินของสหราชอาณาจักร จัดทำ DNO list และแบ่งปันข้อมูลกับผู้ให้บริการต่าง ๆ ตั้งแต่ปี ๒๐๑๙ ซึ่งเลขหมายที่อยู่ในรายการที่หน่วยงานต่าง ๆ รายงานเข้ามาโดยมากเป็นเลขหมายที่ถูกปลอมแปลงเป็นหน่วยงานของรัฐ ธนาคาร ซึ่งผู้ให้บริการโทรศัพท์จะดำเนินการบล็อกเลขหมายที่อยู่ในรายงานดังกล่าวโดยทันที ความร่วมมือกับ Stop Scams ซึ่งเป็นหน่วยงานที่รวมผู้เชี่ยวชาญในกิจการโทรคมนาคมและการเงิน ในปี ๒๐๒๑ Stop Scams ได้ร่วมมือกับ Global Cyber Alliance ให้บริการที่เรียกว่า “159 call service” ซึ่งเป็นเลขหมายที่ให้ประชาชนโทรเข้าไปรายงานหากสงสัยว่ากำลังถูกมิจฉาชีพคุกคาม บริการนี้จะให้ช่องทางประชาชนได้ติดต่อธนาคารอย่างปลอดภัยจากมิจฉาชีพ

๓) เพิ่มความตระหนักรู้และร่วมมือกับประชาชน เนื่องจากการป้องกันไม่ให้มิจฉาชีพเข้าถึงประชาชนนั้นไม่สามารถทำได้อย่างเด็ดขาด Ofcom จึงได้มีแนวทางสร้างความตระหนักรู้ให้แก่ประชาชน เช่น ให้ความรู้เรื่องแนวทางรับมือเมื่อได้รับสายหรือข้อความจากมิจฉาชีพ

มีการให้คำปรึกษาผ่านเว็บไซต์ของ Ofcom และสนับสนุนให้มีการให้ความรู้แก่ประชาชนโดยผู้ประกอบการ และสนับสนุนบริการ ๗๗๒๖ ให้ประชาชนช่วยกันรายงานเลขหมายที่สแกมเมอร์ใช้ นอกจากนี้ Ofcom ยังได้มีความร่วมมือกับตำรวจนครลอนดอน (City of London Police) โดยได้มีการให้ข้อมูลความรู้ต่าง ๆ แก่ตำรวจ เพื่อให้ตำรวจสามารถถ่ายทอดคำแนะนำที่ทันสมัย ทั้งลักษณะของการหลอกลวงใหม่ ๆ และวิธีการรับมือที่ถูกต้องแก่ประชาชนได้อีกด้วย

๒.๒ แนวทางการแก้ปัญหาหลอกลวงทางโทรศัพท์และข้อความของหน่วยงานอื่น ๆ

นอกจาก Ofcom แล้ว ยังมีหน่วยงานหลายแห่งทั้งภาครัฐและเอกชนที่ได้ดำเนินการจัดตั้งความร่วมมือและบริการต่าง ๆ เพื่อบรรเทาปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นอย่างจริงจัง ตัวอย่างเช่น The Information Commissioners' Office (ICO) ซึ่งเป็นหน่วยงานที่ทำหน้าที่ในการบังคับใช้กฎหมายคุ้มครองข้อมูลในสหราชอาณาจักร และมีอำนาจในการจัดการกับบริษัทหรือผู้ประกอบการที่มีส่วนในการนำข้อมูลส่วนบุคคลของประชาชนไปใช้อย่างผิดกฎหมาย หรือมีการปลอมแปลง ในช่วงปี ๒๐๒๑ - ๒๐๒๒ ICO ได้ลงโทษบริษัทที่ส่งข้อความหรืออีเมลรบกวนประชาชนด้วยการปรับไปแล้วกว่า ๒๖ ครั้งเป็นมูลค่า ๒,๔๖๕,๐๐๐ ปอนด์ ปัจจุบัน ICO ได้จัดตั้งพันธมิตรกับหน่วยงานกำกับดูแลและผู้ประกอบการต่าง ๆ ภายใต้ชื่อ Operation Linden เพื่อจัดการปัญหาอย่างจริงจังด้วย (ICO, 2020) นอกจาก ICO ที่เป็นหน่วยงานหลักในการแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นแล้ว ยังมี Action Fraud ซึ่งเป็นศูนย์รับเรื่องร้องเรียนปัญหาการอาชญากรรมออนไลน์ (Cybercrime) รวมถึงปัญหาการหลอกลวง เข้ามาทำหน้าที่ช่วยเหลือผู้ได้รับความเสียหายจากมิจฉาชีพด้วย

ภาคเอกชนหรืออุตสาหกรรมที่เกี่ยวข้องก็ได้มีแนวทางในการจัดการปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นเช่นกัน โดยกลุ่มผู้ให้บริการได้ร่วมลงนามในสัญญา The Telecommunications Fraud Sector Charter (the Fraud Charter) ซึ่งเป็นการทำสัญญาร่วมกันว่าจะให้ความร่วมมือกับรัฐบาลในการจัดการกับผู้กระทำผิด และกลุ่มความร่วมมือนี้ยังได้มีการริเริ่มการดำเนินการต่าง ๆ เช่น มีการสังเกตการณ์อย่างใกล้ชิดกับการแอบอ้างตัวตนเพื่อใช้เลขหมายอย่างผิดกฎหมาย (SIM swap fraud) แบบทันต่อเวลา เพื่อช่วยสถาบันการเงินติดตามการเข้าไปใช้ซิมและการทำธุรกรรมทางการเงิน แบ่งปันข้อมูล และให้ความช่วยเหลือเหยื่อโดยจะทำงานร่วมกันอย่างใกล้ชิดกับกลุ่มให้ความช่วยเหลือเหยื่อเพื่อให้ได้รับหาทางที่ดีที่สุดในการรับมือกับปัญหา นอกจากนี้ผู้ประกอบการยังได้มีการเสนอให้มีการจำกัดจำนวนข้อความที่สามารถส่งได้ จำกัดจำนวนซิมการ์ดที่จำหน่ายผ่านช่องทางออนไลน์ และสังเกตจำนวนการโทรออกของเลขหมายต่าง ๆ ที่โทรหาเลขหมายไม่ซ้ำกัน ซึ่งอาจสงสัยได้ว่าเป็นเลขหมายที่มิจฉาชีพใช้ในการหลอกลวงประชาชนอยู่

๓. ออสเตรเลีย

ออสเตรเลียเป็นประเทศที่มีปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นมากประเทศหนึ่ง จากข้อมูลของ Australian Competition & Consumer Commission (ACCC) ซึ่งเป็นหน่วยงานกำกับดูแลด้านการแข่งขันทางการค้าและคุ้มครองผู้บริโภค พบว่าในปี ๒๐๒๑ พบว่าประชาชนมีการสูญเสียเงินให้กับมิจฉาชีพกว่า ๒ พันล้านดอลลาร์ออสเตรเลีย และคาดว่ามูลค่าความสูญเสียที่ประเมินได้ในปี ๒๐๒๒ จะเพิ่มขึ้นเป็น ๔ ล้านดอลลาร์ออสเตรเลียเนื่องจากจำนวนรายงาน

ผู้เสียหายเพิ่มขึ้นจากปี ๒๐๒๑ ที่รายงานเข้ามายัง Scamwatch สูงขึ้นมากเมื่อเทียบกับปีก่อน (ACCC, 2022) ปัจจุบัน หลายหน่วยงานในออสเตรเลียได้เข้ามามีบทบาทในการแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นทั้งจากหน่วยงานรัฐซึ่งรวมถึงหน่วยงานกำกับดูแลด้านโทรคมนาคม และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง โดยมีรายละเอียดดังนี้

๓.๑ แนวทางการแก้ปัญหาหลอกลวงทางโทรศัพท์และข้อความของหน่วยงานกำกับดูแลในกิจการโทรคมนาคม

หน่วยงานกำกับดูแลด้านกิจการโทรคมนาคมของออสเตรเลียคือ Australian Communications and Media Authority (ACMA) ซึ่งได้มีแนวทางในการแก้ไขปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นตั้งแต่ปี ๒๐๐๓ โดยได้มีการใช้ The Spam Act 2003 ซึ่งกำหนดว่า ผู้ส่งข้อมูลใด ๆ ที่เป็นการโฆษณาประชาสัมพันธ์การตลาดต้องได้รับความยินยอมจากผู้รับ และต้องส่งช่องทางในการปฏิเสธหากไม่ต้องการรับข้อความ หากผู้ส่งข้อความไม่ปฏิบัติตามกฎกติกาดังกล่าว ผู้บริโภคสามารถร้องเรียนมายัง ACMA ได้ (ACMA, n.d.) ต่อมาในปี ๒๐๑๙ ACMA ได้มีการทำแผนการดำเนินการ “Combating Scam Action Plan” ซึ่งแผนการโดยสามารถแบ่งออกได้เป็น ๓ ส่วนและมีกำหนดเวลาการดำเนินการ (ACMA, 2019) ดังนี้

๑) ก่อตั้งคณะทำงานเพื่อการดำเนินการจัดการปัญหาการหลอกลวงในกิจการโทรคมนาคม คณะทำงานนี้มีหน้าที่ให้ความร่วมมือกับทั้งหน่วยงานของรัฐและภาคอุตสาหกรรม รวมทั้งให้ความเห็นในประเด็นกลยุทธ์การบรรเทาปัญหาการหลอกลวง โดยมีกำหนดให้แล้วเสร็จในไตรมาสสุดท้ายของปี ๒๐๑๙ คณะทำงานดังกล่าวจะประกอบด้วยผู้แทนจากทั้งภาครัฐและเอกชน รวมทั้งหน่วยงานในต่างประเทศด้วย เช่น Ofcom ของสหราชอาณาจักร และ FCC ของสหรัฐอเมริกา เนื่องจากปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นสามารถนับได้ว่าเป็นปัญหาระหว่างประเทศเพราะมิจฉาชีพจำนวนมากใช้การโทรออกข้ามประเทศเข้ามายังออสเตรเลีย

๒) กำหนดข้อบังคับให้ผู้ให้บริการในกิจการโทรคมนาคมดำเนินการ โดยมีกำหนดให้แล้วเสร็จในไตรมาสที่ ๒ ของปี ๒๐๒๐ ข้อกำหนดมีดังนี้

๒.๑) แบ่งปันข้อมูลที่เกี่ยวกับมิจฉาชีพระหว่างผู้ประกอบการ การแบ่งปันข้อมูลทำให้ผู้ประกอบการได้รับข้อมูลที่มากเพียงพอที่จะดำเนินการบล็อกเลขหมายที่เป็นมิจฉาชีพได้ง่ายขึ้น โดยการกำหนดข้อบังคับนี้มีความเกี่ยวข้องกับกฎหมายที่มีอยู่คือ Telecommunications Act 1997 ซึ่งกำหนดให้ผู้ให้บริการในกิจการโทรคมนาคมจะต้องป้องกันเครือข่ายของตนจากการกระทำผิดกฎหมาย และให้ความร่วมมือกับเจ้าหน้าที่และหน่วยงานของรัฐอย่างเพียงพอ เพื่อให้เจ้าหน้าที่รัฐสามารถดำเนินการตามกฎหมายและลงโทษผู้กระทำผิดได้

๒.๒) ดำเนินการตรวจสอบ ติดตาม และบล็อกเลขหมายมิจฉาชีพนำไปใช้

๒.๓) ป้องกันเครือข่ายมิให้มีการเข้าถึงของเลขหมายที่ปลอมแปลงโดยมิจฉาชีพภายในประเทศ รวมถึงการปลอมแปลง CLI ด้วย

๒.๔) ป้องกันเครือข่ายมิให้มีการเข้าถึงของเลขหมายที่ปลอมแปลงหรือปลอมแปลงข้อมูลระบุตัวตนโดยมิจฉาชีพที่ในต่างประเทศ

๒.๕) ส่งต่อหรือรายงานเลขหมายที่เป็นมิจฉาชีพหรือผู้กระทำผิดไปยังหน่วยงานของรัฐที่เกี่ยวข้อง เช่น สำนักงานตำรวจสหพันธ์ออสเตรเลีย (Australian Federal Police:

AFP) ศูนย์รายงานและวิเคราะห์การทำธุรกรรมแห่งออสเตรเลีย (Australian Transaction Reports and Analytics Centre: AUSTRAC) สำนักงานคณะกรรมการข่าวกรองอาชญากรรมแห่งออสเตรเลีย (Australian Criminal Intelligence Commission: ACIC) สำนักงานคณะกรรมการกำกับหลักทรัพย์และการลงทุนแห่งออสเตรเลีย (Australian Securities and Investment Commission: ASIC) และยังสามารถส่งเรื่องเข้ามาที่ ACMA ด้วย

๒.๖) นำเทคโนโลยีการคัดครองข้อความสั้น (SMS filtering technology) เข้ามาใช้และให้มีการอัพเดทให้ทันสมัยอยู่เสมอ

๒.๗) ติดตามการพัฒนาทางด้านเทคโนโลยีที่สามารถนำมาใช้กับการแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้น ทั้งในประเทศและในต่างประเทศ เช่น การใช้ระบบข้อมูล CLI ของสหราชอาณาจักรและแคนาดา การใช้ระบบ STIR/SHAKEN ของสหรัฐอเมริกา เป็นต้น

๒.๘) ให้ข้อมูลและคำแนะนำแก่ผู้ใช้บริการ ได้มีการกำหนดให้ผู้ให้บริการโทรศัพท์เคลื่อนที่ต้องให้ข้อมูลเกี่ยวกับการหลอกลวงแก่ผู้ใช้บริการผ่านช่องทางการสื่อสารต่าง ๆ เช่น บนเว็บไซต์ ข้อความสั้น สื่อโซเชียลมีเดีย นอกจากนี้ ยังมีการให้คำปรึกษาทางด้านจิตใจด้วย เช่น องค์กร Life After Scams ซึ่งเป็นหน่วยงานการกุศลที่มีจุดประสงค์ในการช่วยเหลือเหยื่อในด้านจิตใจ

๓) การให้ผู้ประกอบการได้ริเริ่มและทดสอบแนวทางในการลดปัญหาการหลอกลวงผ่านโทรศัพท์และข้อความ โดยมีกำหนดแล้วเสร็จในปี ๒๐๑๙ – ๒๐๒๐

๓.๑) การใช้ Do Not Originate list

๓.๒) ให้เริ่มมีการจัดการกับการหลอกลวงแบบ Wangiri หรือการหลอกลวงโดยการโทรไปยังเป้าหมายโดยให้มีการเรียกเข้าเพียงครั้งเดียว เพื่อให้เป้าหมายโทรกลับ ซึ่งจะทำให้เป้าหมายสูญเสียเงินได้ ผู้ประกอบการจะต้องเข้ามาระบุเลขหมายที่มิจฉาชีพใช้ในการหลอกลวงดังกล่าวและบล็อกเลขหมายนั้น ๆ

๓.๓) บล็อกทราฟฟิกของเลขหมายที่น่าสงสัยว่าเป็นมิจฉาชีพโดยสังเกตจากการโทรออกในปริมาณมากผิดปกติ

๓.๒ แนวทางการแก้ปัญหาหลอกลวงทางโทรศัพท์และข้อความของหน่วยงานอื่น ๆ

หน่วยงานกำกับดูแลด้านการแข่งขันทางการค้าและการคุ้มครองผู้บริโภค หรือ ACCC เป็นอีกหน่วยงานหนึ่งของออสเตรเลียที่มีการดำเนินการเพื่อแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความอย่างจริงจัง ACCC ได้จัดตั้งหน่วยงานย่อยที่ชื่อ Scamwatch ขึ้นเพื่อทำหน้าที่ในการให้ข้อมูลเกี่ยวกับการหลอกลวงประเภทต่าง ๆ แก่ประชาชน เพื่อให้ประชาชนรู้ทันการหลอกลวงและเข้าใจวิธีการรับมือที่ถูกต้อง รวมทั้งมีช่องทางให้ประชาชนผู้ได้รับความเสียหายรายงานเข้ามาเพื่อรับความช่วยเหลือ

นอกจาก ACCC แล้ว ยังมีหน่วยงาน The Australian Cybercrime Online Reporting Network (ACORN) ที่เปิดช่องทางให้ผู้ได้รับความเสียหายร้องเรียนเกี่ยวกับอาชญากรรมออนไลน์ซึ่งรวมถึงการหลอกลวงผ่านช่องทางการสื่อสารต่าง ๆ ด้วย

๔. สิงคโปร์

สิงคโปร์เป็นอีกหนึ่งประเทศที่กำลังประสบกับปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นและปัญหาก็มีแนวโน้มที่จะรุนแรงมากขึ้น ในปี ๒๐๒๒ พบว่ามีกรณีการหลอกลวงทั้งสิ้น ๓๑,๗๒๘ กรณีซึ่งคิดเป็นมูลค่าความสูญเสียกว่า ๖๖๐.๗ ล้านดอลลาร์ โดยเฉพาะการหลอกลวงที่กำลังเพิ่มจำนวนขึ้นอย่างมากที่ชื่อว่า “Fake friend call scams” หรือการหลอกว่าเป็นเพื่อนของเป้าหมายที่ห่างหายจากการติดต่อไปนาน และขอร้องให้เป้าหมายโอนเงินให้ โดยในปี ๒๐๒๒ พบว่ามีกรณีการถูกหลอกในลักษณะดังกล่าวมากถึง ๒,๑๐๖ กรณีซึ่งคิดเป็นมูลค่าความเสียหายกว่า ๘.๘ ล้านดอลลาร์ และพบว่าจำนวนการหลอกลวงเพิ่มมากขึ้นจากปีก่อนหน้าที่มีเพียง ๖๘๖ กรณี (Chua & Sun, 2022) และที่น่าสนใจคือผู้เสียหายที่มีอายุระหว่าง ๒๐ – ๓๙ ตกเป็นผู้เสียหายจากการถูกหลอกลวงมากที่สุด (Tham, 2023) เมื่อพิจารณาในประเด็นเรื่องการรับมือของหน่วยงานต่าง ๆ ของสิงคโปร์นั้น พบว่าประเด็นการหลอกลวงเป็นประเด็นสำคัญในสิงคโปร์ตั้งแต่ปี ๒๐๑๖ และได้มีการดำเนินการต่าง ๆ จากหลายหน่วยงาน โดยมีรายละเอียดดังนี้

๔.๑ แนวทางการแก้ปัญหาหลอกลวงทางโทรศัพท์และข้อความของหน่วยงานกำกับดูแลในกิจการโทรคมนาคม

หน่วยงานกำกับดูแลด้านกิจการโทรคมนาคมของสิงคโปร์หรือ The Infocomm Media Development Authority (IMDA) ได้มีแนวทางการรับมือกับปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นในฐานะหน่วยงานของรัฐตั้งแต่การให้มีการบล็อกเลขหมายที่สแกมเมอร์ปลอมแปลงเป็นเลขหมายของหน่วยงานต่าง ๆ ตั้งแต่ปี ๒๐๑๙ การให้มีการใส่เครื่องหมาย + ด้านหน้าเลขหมายที่มีการโทรเข้าเพื่อเตือนให้ประชาชนระมัดระวังว่าสายที่เรียกเข้าอาจเป็นมิจฉาชีพ ซึ่งแนวทางนี้มีการใช้ตั้งแต่ปี ๒๐๒๐ การบล็อกเลขหมาย Robocall โดยใช้เทคโนโลยีต่าง ๆ ตั้งแต่ปี ๒๐๒๐ และบล็อกเลขหมายปลอมแปลงทั้งเลขหมายบริการโทรศัพท์ประจำที่และเคลื่อนที่ตั้งแต่ปี ๒๐๒๒

แนวทางการจัดการปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นล่าสุดของ IMDA คือให้มีระบบการลงทะเบียนผู้ส่งข้อความสั้น (SMS Sender ID Registry: SSIR) โดยเฉพาะผู้ส่งที่เป็นองค์กร ผู้ส่งที่เป็นองค์กรจะต้องลงทะเบียนยืนยันตัวตนก่อน จึงจะสามารถส่งข้อความไปถึงผู้รับได้ หากผู้ไม่ได้ลงทะเบียนไว้ ข้อความสั้นที่ส่งไปยังผู้รับจะมีสัญลักษณ์เตือนว่าอาจเป็นข้อความหลอกลวงได้ หรือ “Likely-SCAM” เพื่อให้ผู้รับระวังว่าอาจได้รับข้อความจากมิจฉาชีพ โดยหลังจากเดือนกรกฎาคม ๒๐๒๓ หากไม่มีการลงทะเบียนในระบบ SSIR ข้อความทั้งหมดของผู้ส่งที่เป็นองค์กรจะถูกบล็อก โดยล่าสุดในเดือนมกราคม ๒๐๒๓ มีองค์กรกว่า ๑,๒๐๐ แห่งซึ่งใช้ชื่อระบุตัวตนผู้ส่งข้อความสั้น ได้เข้ามาลงทะเบียนในระบบ SSIR แล้ว (IMDA, 2023) ซึ่งรวมทั้งสถาบันทางการเงิน บริษัทขนส่ง ผู้ประกอบการรายย่อย นอกจากนี้ IMDA ยังได้มีการประสานงานกับหน่วยงานต่าง ๆ เพื่อให้เข้ามาลงทะเบียนในระบบ SSIR มากขึ้นด้วย เช่น สมาพันธ์ธุรกิจในสิงคโปร์ (Singapore Business Federation) สมาคมหอการค้าสิงคโปร์ (Singapore International Chamber of Commerce) และกลุ่มธนาคารต่าง ๆ เป็นต้น (IMDA, 2023)

๔.๒ แนวทางการแก้ปัญหาหลอกลวงทางโทรศัพท์และข้อความของหน่วยงานอื่น ๆ

หน่วยงานของรัฐบาลสิงคโปร์ได้จัดตั้ง หน่วยงานชื่อ Scam Alert อยู่ภายใต้สภาป้องกันอาชญากรรมแห่งชาติ (The National Crime Prevention Council) โดย Scam Alert จะทำหน้าที่ในการให้ข้อมูลเกี่ยวกับการหลอกลวงรูปแบบต่าง ๆ แก่ประชาชน และมีการปรับเนื้อหาให้มีความทันสมัยอยู่เสมอ มีการแนะนำวิธีการตรวจสอบว่ากำลังเผชิญอยู่กับมิจฉาชีพหรือไม่ และต้องรับมืออย่างไร นอกจากนี้ ยังทำหน้าที่เป็นช่องทางการรับเรื่องร้องเรียนจากประชาชนด้วย โดยผู้ที่ได้รับการติดต่อจากมิจฉาชีพหรือเป็นผู้เสียหายสามารถติดต่อขอรับคำแนะนำได้ที่หมายเลข ๑๘๐๐-๗๒๒-๖๖๘๘ นอกจาก Scam Alert แล้วยังมีหน่วยงานอื่น ๆ ที่เข้ามาจัดการปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นอีกมากมายตั้งแต่ปี ๒๐๑๗ เช่น Transnational Commercial Crime Task Force ซึ่งเป็นคณะทำงานที่ก่อตั้งขึ้นโดยสำนักงานตำรวจในปี ๒๐๑๗ เพื่อเข้ามาตรวจสอบการหลอกลวงข้ามประเทศ (The Inter-Ministry Committee on Scams: IMCS) ซึ่งก่อตั้งขึ้นในปี ๒๐๒๐ เพื่อจัดการกับปัญหาหลอกลวงโดยได้รวบรวมหน่วยงานที่เกี่ยวข้องมากมายทั้งภาครัฐและเอกชน เช่น กระทรวงมหาดไทยของสิงคโปร์ (Ministry of Home Affairs) กระทรวงการสื่อสารและสารสนเทศ (Ministry of Communications and Information) หน่วยงานกำกับดูแลด้านการเงิน (Monetary Authority of Singapore) ธนาคารต่าง ๆ ผู้ให้บริการโทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต เป็นต้น การจัดทำแอพพลิเคชั่น “Scamshield” โดย สภาป้องกันอาชญากรรมแห่งชาติ (The National Crime Prevention Council) เพื่อช่วยกรองการโทรเข้าและการรับข้อความสั้นที่ไม่พึงประสงค์ นอกจากนี้ยังได้มีการร่วมมือกับหน่วยงานที่ทำหน้าที่เกี่ยวกับการบังคับใช้กฎหมายระหว่างประเทศ โดยแผนกกิจการการค้าของสำนักงานตำรวจ (the Police’s Commercial Affairs Department) ได้จัดตั้งหน่วยป้องกันการหลอกลวง (The Anti-Scam Division: ASD) ขึ้นเพื่อดำเนินการด้านนี้โดยตรงในปี ๒๐๒๑

๕. ข้อสรุปแนวทางการแก้ปัญหาของหน่วยงานที่เกี่ยวข้องในต่างประเทศ

จากการศึกษาแนวทางในการแก้ปัญหาของหน่วยงานที่เกี่ยวข้องในต่างประเทศ พบว่าหลายประเทศทมีแนวทางที่คล้ายคลึงกัน ซึ่งแนวทางดังกล่าวสามารถสรุปได้ดังนี้

๕.๑ การใช้เทคโนโลยีในการป้องกันการเข้าถึงประชาชนของมิจฉาชีพ เนื่องจากปัจจุบันมิจฉาชีพได้ใช้เทคโนโลยีในการเข้าถึงเป้าหมายมากขึ้น เช่นการใช้ Robocall การปลอมแปลงเลขหมาย หรือแม้แต่ข้อมูลระบุตัวตน ดังนั้น หลายหน่วยงานจึงใช้เทคโนโลยีเข้ามาช่วยในการสกัดกั้นสายเรียกเข้าและข้อความจากมิจฉาชีพ รวมทั้งบล็อกเลขหมายของมิจฉาชีพด้วย โดยเทคโนโลยีที่นำมาใช้มักเป็นเทคโนโลยีที่ช่วยระบุตัวตนของผู้โทร เช่น CLI ที่มีการใช้ในสหราชอาณาจักร และ STIR/SHAKEN ของสหรัฐอเมริกา และยังมีเทคโนโลยีที่ใช้ในการคัดกรองข้อความสั้นที่อาจเป็นมิจฉาชีพ (SMS Filtering) ของสิงคโปร์ เป็นต้น

๕.๒ การใช้กฎเกณฑ์ข้อบังคับที่เป็นรูปธรรมและมีบทลงโทษที่ชัดเจน การใช้เทคโนโลยีเพื่อสกัดกั้นมิจฉาชีพนั้น หน่วยงานของรัฐหลายแห่งโดยเฉพาะหน่วยงานกำกับดูแลในกิจการโทรคมนาคมต้องมีกฎเกณฑ์บังคับหรือใช้กฎหมายร่วมด้วยเพื่อให้มีการนำไปใช้อย่างจริงจัง เช่น สหราชอาณาจักรที่มีการใช้กฎหมาย The Communications Act เข้ามาร่วมด้วย หรือ

สหรัฐอเมริกาที่กำหนดเกณฑ์การใช้ STIR/SHAKEN ในระบบของผู้ให้บริการโทรศัพท์เคลื่อนที่ โดยหากผู้ประกอบการไม่ให้ความร่วมมือก็จะมีการลงโทษอย่างชัดเจน เช่น การบล็อกทราฟฟิกจากผู้ให้บริการนั้น ๆ การปรับเป็นเงิน เป็นต้น นอกจากการใช้กฎหมายเพื่อบังคับให้มีการใช้เทคโนโลยีแล้วนั้น ยังมีการใช้กฎหมายเพื่อลงโทษผู้กระทำผิดหรือสแกมเมอร์อีกด้วย ดังเช่นตัวอย่างในสหรัฐอเมริกาที่มีการปรับด้วยเงินจำนวนที่สูงมากกับบริษัทที่มีการใช้ Robocall

๕.๓ การอาศัยความร่วมมือของหน่วยงานที่เกี่ยวข้อง ทั้งหน่วยงานกำกับดูแลในกิจการโทรคมนาคมและหน่วยงานอื่น ๆ ทั้งภาครัฐและเอกชน เนื่องจากปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นเป็นปัญหาที่เกี่ยวข้องกับหลายหน่วยงาน และต้องใช้ข้อมูลและความชำนาญเฉพาะทางจากหลายส่วนประกอบกัน เพราะฉะนั้น ความร่วมมือกันในรูปแบบต่าง ๆ จึงเป็นแนวทางที่ช่วยให้สามารถแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความสั้นได้อย่างรอบด้าน ในหลายประเทศก็มีการก่อตั้งความร่วมมือกันทั้งจากภาครัฐและเอกชน เพื่อให้มีการแบ่งปันข้อมูลอย่างเพียงพอต่อการแก้ปัญหาการหลอกลวงทางโทรศัพท์และข้อความอย่างเป็นระบบ มีการใช้ทักษะความชำนาญเฉพาะทางของบางหน่วยงานมาร่วมด้วย เช่น การร่วมมือกับหน่วยงานด้านการเงิน การธนาคาร ผู้ประกอบการในอุตสาหกรรม นอกจากการร่วมมือกันระหว่างภาคส่วนต่าง ๆ ในประเทศแล้ว ยังมีการร่วมมือกันระหว่างประเทศด้วย เพราะมิจฉาชีพจำนวนมากใช้การโทรระหว่างประเทศเข้าไปยังเป้าหมายที่อยู่ในต่างประเทศ ซึ่งโดยปกติแล้วอำนาจของประเทศที่ได้รับความเสียหายจะไม่สามารถเข้าไปดำเนินคดีผู้กระทำผิดในต่างประเทศได้ ด้วยเหตุนี้ การร่วมมือระหว่างประเทศจึงเป็นอีกแนวทางหนึ่งที่จะช่วยลดปัญหาการหลอกลวงทางโทรศัพท์และข้อความลงได้

๕.๔ การสร้างความตระหนักรู้แก่ประชาชน แม้ว่าการหลอกลวงจะเน้นโจมตีที่จุดอ่อนของความเป็นมนุษย์ซึ่งเป็นจุดที่แก้ไขได้ยาก แต่การสร้างความตระหนักรู้และให้ประชาชนได้เฝ้าระวังตนเองจากมิจฉาชีพก็ยังเป็นสิ่งที่จำเป็น โดยนอกจากประชาชนจะได้ระวังตนเองแล้วนั้น การที่ประชาชนมีความรู้ความเข้าใจก็จะสามารถรับมือกับสถานการณ์เมื่อถูกคุกคามจากมิจฉาชีพหรือเมื่อตกเป็นผู้เสียหายไปแล้ว เช่น ทราบว่าจะต้องไปร้องเรียนที่ไหน ดำเนินการอย่างไร และจะสามารถแบ่งปันข้อมูลเพื่อให้คนอื่นไม่ตกเป็นผู้เสียหายได้อย่างไร เป็นต้น

ข้อสรุปประการหนึ่งที่สำคัญจากการศึกษากรณีการแก้ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์และข้อความสั้นในต่างประเทศคือ การต้องมีแนวทางที่แก้ปัญหาแบบบูรณาการโดยหน่วยงานที่รับผิดชอบหลายส่วนต้องมีส่วนร่วมในการแก้ปัญหา ดังที่ได้มักมีการกล่าวว่า “There is no silver bullet to stop scams” (ACMA, 2022) หรือ “ไม่มีแนวทางใดจะแก้ปัญหาการหลอกลวงได้โดยง่าย” ซึ่งจากการศึกษาแนวทางในการแก้ปัญหานั้น พบว่าแต่ละประเทศมีแนวทางในการแก้ปัญหาหลายขั้นตอนและต้องอาศัยความร่วมมือของหน่วยงานทั้งภาครัฐและเอกชน สำหรับกรณีของประเทศไทยก็เช่นเดียวกัน ควรมีการใช้แนวทางการแก้ปัญหาโดยมุ่งเน้นไปที่ส่วนต่าง ๆ ของปัญหาอย่างรอบด้านทั้งจากฝั่งผู้กระทำผิด จากฝั่งผู้เสียหาย และผู้ที่มีโอกาสตกเป็นผู้เสียหายซึ่งก็คือประชาชนทั่วไป เพื่อให้การแก้ปัญหาประสบผลสำเร็จซึ่งจะส่งผลดีต่อคุณภาพชีวิตของประชาชนตามเป้าหมายที่ตั้งไว้ในยุทธศาสตร์ชาติ

กรอบแนวคิดของการวิจัย

สรุป

จากการศึกษาแนวคิด ทฤษฎี และวรรณกรรมข้อมูลทั่วไปที่เกี่ยวข้อง พบว่ามีการอธิบายลักษณะการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่รวมทั้งผ่านช่องทางการสื่อสารอื่น ๆ เป็นจำนวนมากเนื่องจากปัญหาดังกล่าวเป็นปัญหาที่มีความรุนแรงและเป็นปัญหาร่วมในหลายประเทศ โดยงานศึกษามีทั้งการอธิบายหลักการต่าง ๆ ที่ผู้กระทำผิดใช้ในการหลอกลวง ซึ่งมักเป็นหลักการที่ใช้โจมตีจุดอ่อนของมนุษย์ เช่น การใช้ความต้องการพื้นฐานของมนุษย์ การบีบบังคับให้ผู้เสียหายหลงกลในเวลาจำกัด และการใช้ความน่าเชื่อถือของหน่วยงานรัฐในการหลอกลวงผู้เสียหาย ในขณะเดียวกัน

มีงานศึกษาหลายชิ้นที่อธิบายในเชิงจิตวิทยาจากฝั่งผู้เสียหาย โดยการตกเป็นผู้เสียหายนั้นก็เป็นจุดอ่อนของมนุษย์เช่นเดียวกัน ด้วยเหตุข้างต้นนี้ ประกอบกับการพัฒนาทางด้านเทคโนโลยี โดยเฉพาะเทคโนโลยีในกิจการการสื่อสารและโทรคมนาคม ทำให้ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มีความรุนแรงและส่งผลกระทบในวงกว้าง เมื่อพิจารณาปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในเชิงสังคมจิตวิทยาข้างต้นแล้วนั้น จะเห็นได้ว่าเป็นสิ่งที่ไม่สามารถป้องกันได้ด้วยการให้ความรู้หรือความตระหนักรู้แก่ประชาชนเพียงอย่างเดียว จำเป็นจะต้องมีระบบการปกป้องประชาชนด้วยวิธีการต่าง ๆ ประกอบกัน ในงานวิจัยชิ้นนี้จึงมีการศึกษาแนวทางในการแก้ไขปัญหารวมทั้งแนวทางการป้องกันปัญหาที่จะเกิดขึ้น โดยใช้การศึกษาจากกรณีตัวอย่างในประเทศด้วย ซึ่งจากการศึกษาดังกล่าว สามารถกล่าวได้ว่าการแก้ไขปัญหานั้นควรเป็นแบบ “บูรณาการ” กล่าวคือ ควรมีแนวทางในการแก้ไขปัญหาอย่างรอบด้าน ทั้งการแก้ไขปัญหาทั้งฝั่งผู้กระทำผิดคือมีการป้องกันการเข้าถึงประชาชนของผู้กระทำผิดโดยการใช้เทคโนโลยี การมีบทลงโทษที่ชัดเจน การแก้ไขปัญหาจากฝั่งผู้เสียหายหรือเป้าหมายให้มีความตระหนักรู้และเข้าใจการหลอกลวง รวมทั้งทราบถึงช่องทางในการร้องเรียนในกรณีที่มีการคุกคามจากมิจฉาชีพ นอกจากนี้ ยังควรมีการแก้ไขปัญหาโดยอาศัยความร่วมมือของหน่วยงานต่าง ๆ ที่เกี่ยวข้อง ทั้งหน่วยงานของรัฐ หน่วยงานเอกชน ผู้เชี่ยวชาญในด้านต่าง ๆ เป็นต้น ทฤษฎี แนวคิด และวรรณกรรมที่เกี่ยวข้องที่ได้นำเสนอในบทนี้จะมีการนำไปประยุกต์ใช้ในการอธิบายลักษณะการกระทำผิดในกรณีของประเทศไทย และแนวทางการศึกษาในต่างประเทศจะได้มีการนำมาใช้เปรียบเทียบกับมาตรการในประเทศไทยตามแนวทางการศึกษาข้อวิเคราะห์ช่องว่าง (Gap Analysis) ซึ่งเป็นระเบียบวิธีวิจัยที่ใช้ในงานวิจัยชิ้นนี้ด้วย โดยผลการศึกษาเปรียบเทียบจะได้มีการนำเสนอในลำดับต่อไป

บทที่ ๓
พฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่และผลกระทบที่เกิดขึ้น

เนื่องจากปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยเป็นปัญหาที่สร้างผลกระทบเป็นอย่างมากทั้งในระดับประชาชน สังคม และประเทศชาติรวมทั้งความมั่นคง การศึกษาในกรณีของประเทศไทยจึงเป็นสิ่งจำเป็นและเป็นประโยชน์อย่างยิ่งในการนำเสนอแนวทางแก้ไขปัญหาที่เหมาะสม ในงานวิจัยชิ้นนี้ จึงมีการศึกษาทั้งพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่หรือลักษณะการกระทำผิด ผลกระทบที่เกิดขึ้น และแนวทางในการแก้ไขและรับมือกับปัญหาดังกล่าวของหน่วยงานที่เกี่ยวข้องในปัจจุบัน โดยข้อมูลที่ใช้ในการศึกษานั้นมาจาก ๒ ส่วน คือข้อมูลปฐมภูมิ และข้อมูลทุติยภูมิ โดยข้อมูลปฐมภูมิได้จากการสัมภาษณ์เชิงลึก (In-depth interview) กับหน่วยงานที่เกี่ยวข้อง ได้แก่

๑. เจ้าหน้าที่ตำรวจ โดยได้มีการสัมภาษณ์กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) ซึ่งเป็นหน่วยงานที่รับผิดชอบเกี่ยวกับการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

๒. ผู้แทนในคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งค์โทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง โดยได้มีการสัมภาษณ์ ๒ กลุ่มย่อยซึ่งเป็นองค์ประกอบของคณะทำงานดังกล่าว ได้แก่ กลุ่มหน่วยงานของรัฐ และหน่วยงานเอกชน ดังนี้

๒.๑ หน่วยงานของรัฐ ประกอบด้วยสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) ในฐานะหน่วยงานกำกับดูแลด้านกิจการโทรคมนาคม และธนาคารแห่งประเทศไทย (ธปท.) ในฐานะหน่วยงานกำกับดูแลสถาบันการเงินในประเทศไทย

๒.๒ หน่วยงานเอกชน ประกอบด้วยบริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัท เมลบิท เอเชีย แปซิฟิค จำกัด ในฐานะผู้ให้บริการในกิจการโทรคมนาคม

ในส่วนของข้อมูลทุติยภูมินั้น ได้มีการค้นคว้าข้อมูลจากเอกสารข้อมูลที่เกี่ยวข้อง (Documentary Research) เช่น รายงานคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งโทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง เอกสารและรายงานที่เปิดเผยต่อสาธารณะของธนาคารแห่งประเทศไทย และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี เป็นต้น

เมื่อได้รับข้อมูลครบถ้วนแล้ว จึงนำข้อมูลทั้งหมดมาประมวลเพื่ออธิบายพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ผลกระทบที่เกิดขึ้น รวมทั้งมาตรการต่าง ๆ ของหน่วยงานที่เกี่ยวข้อง โดยมีรายละเอียดดังที่จะได้นำเสนอต่อไป ทั้งนี้ เนื้อหาที่นำเสนอในบทนี้จะเป็นข้อมูลที่ได้รวบรวมและเรียบเรียงแล้ว ในส่วนของรายละเอียดการสัมภาษณ์ของแต่ละหน่วยงานจะได้มีการนำเสนอในภาคผนวกของงานวิจัยต่อไป

รูปแบบและพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

๑. ลักษณะทั่วไปของพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่จัดเป็นอาชญากรรมทางเทคโนโลยีรูปแบบหนึ่ง บช. สอท. ได้ให้ความหมายของการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (Call Center) ว่า “...เป็นคดีที่ใช้สังคมออนไลน์ โทรศัพท์ หรือโทรผ่านระบบอินเทอร์เน็ต (Voice over Internet Protocol หรือ VoIP) สุ่มติดต่อไปยังผู้เสียหาย สร้างเรื่องหลอกลวงและให้ผู้เสียหายมีการโอนเงินให้” (บช.สอท., ๒๕๖๖, หน้า ๑) การหลอกลวงผ่านเครือข่ายโทรศัพท์ยังคงมีหลักการในการหลอกลวงและมีจุดประสงค์เช่นเดียวกันกับอาชญากรรมอื่น ๆ แต่ดั้งเดิม เช่น การฉกชิงวิ่งราว เป้าหมายประการสำคัญที่สุดคือการได้ไปซึ่งทรัพย์สินของมีค่าของผู้อื่น เมื่อมีการพัฒนามากขึ้นของเทคโนโลยี โดยเฉพาะอย่างยิ่งเทคโนโลยีในการติดต่อสื่อสาร ก็ทำให้อาชญากรรมเหล่านี้ได้ปรับเปลี่ยนรูปแบบไปโดยเข้าถึงผู้คนหรือเป้าหมายของมิจฉาชีพได้อย่างสะดวก รวดเร็ว ในต้นทุนที่ประหยัดได้มากขึ้น หรืออาจกล่าวได้ว่า อาชญากรสมัยใหม่ได้พึ่งพาอาศัยเทคโนโลยีในการก่ออาชญากรรม อีกทั้งเทคโนโลยีใหม่ในปัจจุบันโดยเฉพาะเรื่องการเงินและธนาคารมีความทันสมัย ทางธนาคารได้ออกแบบระบบต่าง ๆ เพื่ออำนวยความสะดวกทำให้มีการทำธุรกรรมทางการเงินได้แบบรวดเร็ว ทำให้มีการสูญเสียทรัพย์ให้แก่มิจฉาชีพได้ในเวลารวดเร็วเช่นกัน จึงเป็นสาเหตุสำคัญที่ทำให้ปัญหาหลอกลวงผ่านเครือข่ายโทรศัพท์ขยายตัวอย่างมากในปัจจุบัน

ประเทศไทยนับได้ว่ากำลังประสบปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่อย่างมาก โดยข้อมูลจาก บช.สอท. (๒๕๖๖) พบว่า จากวันที่ ๑ มีนาคม ๒๕๖๕ ถึงวันที่ ๑๘ มีนาคม ๒๕๖๖ ปัญหาดังกล่าวได้มีจำนวนการร้องเรียนผ่านช่องทางการแจ้งความออนไลน์ของ บช.สอท. ถึง ๒๐,๕๒๕ กรณี หรือคิดเป็นร้อยละ ๙.๒๓ ของจำนวนอาชญากรรมทางเทคโนโลยีทั้งหมด นอกจากนี้ จากข้อมูลของ ธปท. พบว่ามีความเสียหายจากการหลอกลวงซึ่งประเมินจากจำนวนเงินที่มีการโอนผ่านช่องทางโมบายแบงก์กิ้ง (Mobile Banking) ในปี ๒๕๖๕ กว่า ๒๗๔ ล้านบาทและมีจำนวนธุรกรรมทางการเงินถึง ๖,๐๐๐ รายการ ด้วยเหตุนี้ จึงมีความจำเป็นต้องศึกษารายละเอียดขององค์ประกอบและขั้นตอนการกระทำผิด โดยผลการศึกษาจากการสัมภาษณ์ จะได้มีการอธิบายในลำดับต่อไป

๑.๑ องค์ประกอบของการกระทำผิด

จากทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) (สุมนทิพย์และคณะ, ๒๕๖๓: หน้า ๓๑) องค์ประกอบและพฤติกรรมการกระทำผิดหรือหลอกลวงสามารถแบ่งออกได้เป็น ๓ ส่วนหลัก คือ มิจฉาชีพหรือผู้กระทำผิด เป้าหมายหรือผู้เสียหาย และโอกาส เมื่อมีครบทั้ง ๓ องค์ประกอบแล้วจึงจะเกิดการกระทำผิดขึ้น โดยเมื่อพิจารณาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแล้วนั้น ก็สามารถแบ่งองค์ประกอบทั้ง ๓ ส่วนได้ดังนี้

๑.๑.๑ มิจฉาชีพหรือผู้กระทำผิด

การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่นั้นมิได้กระทำการโดยมิจฉาชีพเพียงคนเดียว หากแต่เป็นการทำงานร่วมกันของมิจฉาชีพหลายคน หรือที่เรียกว่าทำเป็น

“ขบวนการ” หรือที่เรียกว่าเป็น “แก๊ง” ซึ่งหมายถึง การกระทำผิดร่วมกันของผู้กระทำผิดมากกว่าหนึ่งคนและมีการแบ่งหน้าที่กันทำ โดยขบวนการของมิจฉาชีพหรือผู้กระทำผิดในความผิดการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่นั้นมีลักษณะคล้ายกับองค์กรหรือบริษัทหนึ่ง และยังมีความคล้ายคลึงกับ “แฟรนไชส์” (Franchise) โดยมีระบบการวางคนให้ทำหน้าที่ในตำแหน่งต่าง ๆ มีการศึกษาตลาดเป็นอย่างดีหรือมีการศึกษามาก่อนว่าจริตของคนไทยเป็นอย่างไร ช่วงนี้มีสถานการณ์อะไรในประเทศไทยที่สามารถนำมาปรับใช้กับการหลอกลวงได้ มีสูตรหรือคู่มือสำหรับใช้ในการหลอกลวง มีการวางระบบโยกย้ายเงิน โดยขบวนการดังกล่าว มักประกอบด้วยตำแหน่งหน้าที่ ดังนี้

๑) มิจฉาชีพที่ทำหน้าที่ติดต่อเป้าหมาย มิจฉาชีพกลุ่มนี้จัดว่าเป็นมิจฉาชีพด่านหน้าที่ต้องติดต่อกับเป้าหมาย โดยจะได้รับมอบหมายเป็นผู้ติดต่อพูดคุยกับเป้าหมาย มีหน้าที่ต้องพูดคุยหว่านล้อมเป้าหมายให้มีการโอนเงินให้กับมิจฉาชีพด้วยวิธีการหรือเทคนิคทางจิตวิทยาต่าง ๆ มิจฉาชีพกลุ่มนี้มักเป็นคนชาติเดียวกันกับเป้าหมายของการหลอกลวง ในกรณีของประเทศไทยที่มีการหลอกลวงคนไทยนั้น ก็ต้องใช้มิจฉาชีพที่เป็นคนไทยเพื่อให้สามารถสื่อสารกับคนไทยได้ดี จึงพบว่ามิจฉาชีพกลุ่มนี้ส่วนใหญ่เป็นคนไทย มิจฉาชีพที่ได้รับหน้าที่นี้มักพำนักอยู่นอกราชอาณาจักรไทย เพื่อป้องกันการถูกจับกุมจากเจ้าหน้าที่ตำรวจได้โดยง่าย นอกจากนี้ ยังมีลักษณะการรวมกลุ่มอยู่ด้วยกันในฐานปฏิบัติการเพื่อให้หัวหน้าขบวนการสามารถควบคุมพฤติกรรมการหลอกลวงและยังสามารถป้องกันความลับรั่วไหลได้อีกด้วย

๒) กลุ่มสนับสนุนหรือผู้ดูแลระบบ แม้ว่าผู้กระทำผิดหลักที่มักมีการกล่าวถึงคือมิจฉาชีพที่ทำหน้าที่ติดต่อกับเป้าหมาย ทว่า การกระทำผิดจะไม่สามารถดำเนินการจนสำเร็จได้โดยขาดกลุ่มสนับสนุนหรือผู้ดูแลระบบ กลุ่มนี้เป็นกลุ่มที่มิได้ติดต่อพูดคุยกับเป้าหมายโดยตรง แต่เป็นผู้ดำเนินการจัดหาทรัพยากร เตรียมอุปกรณ์ที่จำเป็น อำนวยความสะดวกต่าง ๆ ให้กับมิจฉาชีพกลุ่มแรก นอกจากนี้ ยังมีกลุ่มสนับสนุนที่ทำหน้าที่เตรียมฉากหลังให้กับมิจฉาชีพกลุ่มแรกเมื่อมีการโทรไปยังเป้าหมายอีกด้วย เช่น การทำเสียงเหมือนผู้โทรอยู่ในสถานีตำรวจ เมื่อมีการแอบอ้างว่าเป็นเจ้าหน้าที่ตำรวจ โดยมีการเปิดเสียงประกอบเป็นวอล์กกี้ทอล์กกี้ เพื่อให้ฟังดูน่าเชื่อถืออีกด้วย อย่างไรก็ดี มีข้อสังเกตว่ากลุ่มสนับสนุนนี้ยังรวมถึงผู้ที่มีความรู้ความสามารถทางเทคนิคและเทคโนโลยีในระดับสูง เนื่องจากการหลอกลวงในบางครั้งได้มีการใช้แอพดูดเงินหรือการควบคุมโทรศัพท์เคลื่อนที่ของเป้าหมายจากทางไกล ซึ่งการทำแอพในลักษณะนี้ต้องใช้ความรู้ความสามารถมาก

๓) นายทุน องค์ประกอบหนึ่งที่สำคัญคือการมีนายทุนที่สนับสนุนค่าใช้จ่ายต่าง ๆ ที่เกิดขึ้น เช่น ค่าจ้างแรงงาน ค่าใช้จ่ายในอุปกรณ์ที่จำเป็น ค่าเช่าสถานที่ในการตั้งฐานปฏิบัติการ เป็นต้น จากข้อมูลในปัจจุบัน การจับกุมถึงนายทุนทำได้ยาก อย่างไรก็ดี มักพบว่าเป็นชาวต่างชาติรวมถึงชาวจีน จึงอาจกล่าวได้ว่า ขบวนการหรือแก๊งคอลเซ็นเตอร์มีลักษณะที่เป็นการรวมกลุ่มของหลายชาติในลักษณะเช่น นายทุนที่เป็นชาวจีน คนโทรหลอกเป้าหมายที่เป็นคนไทย และใช้สถานปฏิบัติการของกัมพูชา เป็นต้น

๑.๑.๒ ผู้เสียหาย

จากข้อมูลการร้องเรียนของ บช. สอท. พบว่าผู้เสียหายในไทยนั้นสามารถเป็นได้ทุกเพศทุกวัย อย่างไรก็ดี ผู้เสียหายมีความแตกต่างกันตามลักษณะหรือเทคนิคในการหลอกลวงของมิจฉาชีพ เช่น ผู้เสียหายที่มีอายุน้อยมักตกเป็นเหยื่อการหลอกลวงแบบหลอกให้ลงทุน

มากกว่าผู้เสียหายที่มีอายุ และผู้เสียหายมักมีฐานะ ขาดความรู้ หรือไม่ได้ติดตามข่าวสาร ทั้งนี้ พบว่ากว่าร้อยละ ๙๐ ของผู้เสียหายต้องการได้เงินคืนเท่านั้น

๑.๑.๓ โอกาส

โดยทั่วไปแล้ว โอกาสของการกระทำผิดมักประกอบด้วยช่วงเวลา (Time) และสถานที่ (Place) เมื่อพิจารณาการกระทำผิดในความผิดหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ โอกาสของการการกระทำผิดอาจมีความแตกต่างจากอาชญากรรมโดยทั่วไป เนื่องจากการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สามารถเกิดขึ้นได้ทุกเวลา โดยผู้กระทำผิดสามารถติดต่อหรือโทรไปยังเป้าหมายในเวลาใดก็ได้ ในส่วนของโอกาสในแง่ของสถานที่ สามารถพิจารณาได้ว่าช่องทางในการเข้าถึงเป้าหมาย โดยเฉพาะเมื่อช่องทางในการติดต่อสื่อสารถูกพัฒนาขึ้นอย่างมากตามการพัฒนาของเทคโนโลยี ยิ่งทำให้โอกาสในการกระทำผิดของมิจฉาชีพเพิ่มมากขึ้นไปด้วย นอกจากนี้ การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่นั้นยังมีโอกาสอีกประการหนึ่งที่สำคัญ คือสภาพแวดล้อมที่เอื้อให้เกิดการกระทำผิดได้ง่ายขึ้น เช่น การอาศัยช่องว่างทางกฎหมายยังไม่ครอบคลุมการการกระทำผิดที่ผู้กระทำผิดอยู่ในต่างประเทศ ทำให้ดำเนินการจับกุมผู้กระทำผิดได้ยาก การอาศัยความสะดวกสบายของ Mobile Banking เป็นต้น

๑.๒ ขั้นตอนการกระทำผิด

เมื่อองค์ประกอบของการกระทำผิดตามทฤษฎีสามเหลี่ยมอาชญากรรมครบถ้วนแล้ว จึงเกิดการกระทำผิดขึ้น โดยการกระทำผิดของการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยมีขั้นตอนตั้งแต่การเตรียมการไปจนถึงการร้องเรียนของผู้เสียหาย ดังนี้

๑.๒.๑ การเตรียมการ

ก่อนการเข้าถึงเป้าหมาย มิจฉาชีพจะต้องมีการจัดเตรียมระบบให้พร้อม เพื่อให้การหลอกลวงเป็นไปโดยรวดเร็ว น่าเชื่อถือ และรอดพ้นจากการจับกุมของเจ้าหน้าที่ตำรวจ โดยแบ่งการเตรียมการที่สำคัญดังนี้

๑) เตรียมสถานที่สำหรับเป็นฐานปฏิบัติการ มิจฉาชีพมักใช้พื้นที่บริเวณชายแดนประเทศเพื่อนบ้าน เช่น กัมพูชา เป็นฐานปฏิบัติการ ด้วยเหตุผลประการสำคัญคือการรอดพ้นจากการบังคับใช้กฎหมายไทย นอกจากนี้ ยังพบว่าบริเวณชายแดนประเทศเพื่อนบ้านยังสามารถใช้ซิมโทรศัพท์ของไทยในการติดต่อเข้ามายังประเทศไทยได้เนื่องจากสัญญาณโทรศัพท์ของไทยครอบคลุมถึง เช่น อรัญประเทศ ตลาดโรงเกลือ ปอยเปต หรือฝั่งตรงข้ามแม่สาย จึงถือเป็นบริเวณที่เอื้ออำนวยให้เกิดการกระทำผิดได้ง่าย

๒) เตรียมช่องทางการเข้าถึงเป้าหมาย

๒.๑) ซิมการ์ด และ "ซิมม้า" หากมิจฉาชีพใช้เบอร์โทรศัพท์ปกติและการโทรผ่านเครือข่ายอินเทอร์เน็ต (Voice over Internet Protocol: VoIP) ในการติดต่อเป้าหมาย จะมีการจัดหาซิมการ์ดเป็นจำนวนมาก แต่ทั้งนี้ เนื่องจากปัจจุบันสำนักงาน กสทช. ได้กำหนดให้มีการลงทะเบียนซิม โดยบุคคลทั่วไปสามารถลงทะเบียนได้ด้วยตนเองหรือที่ลูกตู้ไม่เกิน ๕ ซิม หากต้องการลงทะเบียนมากกว่านั้น จะต้องไปดำเนินการลงทะเบียนที่ศูนย์บริการของผู้ให้บริการโทรศัพท์รายนั้น ๆ ในแง่หนึ่งก็ทำให้มิจฉาชีพลดจำนวนการใช้ซิมการ์ดลง หรืออาจเปลี่ยนวิธีการติดต่อ

เป้าหมายจากการใช้เลขหมายโทรศัพท์ทั่วไปเป็นช่องทางอื่นแทน อย่างไรก็ดี พบว่ามีมิจฉาชีพที่ใช้วิธีการจ้างให้คนอื่นไปลงทะเบียนเลขหมายโทรศัพท์เคลื่อนที่ให้ และมิจฉาชีพจะนำเลขหมายนั้นไปใช้ในการหลอกลวง โดยเรียกซิมการ์ดที่ลงทะเบียนจากบุคคลที่ไม่ได้เป็นผู้ใช้งานซิมการ์ดนั้นว่า “ซิมม้า” ซึ่งซิมม้าเหล่านี้มีการนำไปใช้ร่วมกับบัญชีม้า ที่จะได้อธิบายต่อไปด้วย

๒.๒) GSM Gateways (Simbox) การใช้ GSM Gateways (Simbox) หรือ เครื่องแปลงสัญญาณโทรศัพท์แบบใส่ซิมการ์ด เป็นอุปกรณ์ในการแปลงสัญญาณโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ตเป็นสัญญาณโทรศัพท์เพื่อโทรออกไปหลอกลวงผู้เสียหาย โดยการใช้ Simbox จะทำให้เลขหมายโทรศัพท์ที่ปรากฏยังเป้าหมายเป็นเลขหมายที่เหมือนทำการโทรออกจากประเทศไทย เพื่อให้มีความน่าเชื่อถือมากขึ้น โดยเฉพาะอย่างยิ่งเมื่อมีมาตรการให้ประชาชนเฝ้าระวังและระงับสายเรียกเข้าจากต่างประเทศ มิจฉาชีพจึงหันไปใช้ Simbox กลุ่มมิจฉาชีพจะติดตั้งอุปกรณ์ในประเทศไทยและจัดให้มีผู้ดูแลระบบ ซึ่งทำหน้าที่ตั้งแต่การจัดหาอาคารสถานที่สำหรับติดตั้งอุปกรณ์ โดยจะเช่าพื้นที่ห่างไกลชุมชนเพื่อลดต้นทุน และติดตั้ง Simbox ไว้ โดยมีคนดูแลการทำงานของระบบเพียงไม่กี่คน ซึ่งมักเป็นการเข้ามาตรวจสอบดูเท่านั้นว่าระบบยังใช้งานได้อยู่ ในการจับกุมเจ้าหน้าที่ตำรวจจะใช้เบาะแสปริมาณทราฟฟิก (Traffic) ของข้อมูลที่มากผิดปกติเมื่อเทียบกับพื้นที่โดยรอบ อย่างไรก็ดี แม้ว่าจะมีการจับกุมได้ ก็มักจับกุมได้เฉพาะผู้ดูแลระบบ และยึดของกลางที่เป็น Simbox หรือตัวโครงข่าย Gateway ที่รับสัญญาณมาอีกทอดนึง ซึ่งสามารถสืบไปยังผู้กระทำผิดส่วนอื่นได้ยาก

๒.๓) SMS นอกจากซิมการ์ดแล้ว ยังพบว่ามีการกระทำผิดในลักษณะใกล้เคียงกันคือการส่งข้อความหลอกลวงไปทางบริการข้อความสั้น (SMS) โดยผู้กระทำผิดจะใช้การซื้อ SMS คราวละมาก ๆ (Bulk SMS) จากผู้ให้บริการบางราย โดยปกติแล้วนั้น ค่าบริการข้อความสั้นในประเทศไทยมีราคาที่ค่อนข้างถูก โดยจากรายงานอัตราค่าบริการโทรคมนาคมประจำไตรมาสที่ ๓/๒๕๖๕ ของสำนักงาน กสทช. บริการ SMS มีอัตราค่าบริการเฉลี่ยเพียง ๐.๗๘ บาทต่อข้อความเท่านั้น โดยเมื่อพิจารณาถึงการขายคราวละมาก ๆ ก็จะยิ่งมีราคาที่ถูกลง แม้ว่าบริการข้อความสั้นที่มีราคาถูกจะเป็นประโยชน์ต่อภาคธุรกิจที่จำเป็นต้องใช้บริการข้อความสั้นในการติดต่อกับลูกค้า และเป็นประโยชน์กับประชาชนในการเข้าถึงบริการโทรคมนาคม แต่ก็เป็นช่องว่างให้กับมิจฉาชีพนำไปหลอกลวงประชาชนได้เป็นจำนวนมากเช่นกัน

๓) เตรียมช่องทางการโอนย้ายทรัพย์สิน และการใช้ “บัญชีม้า”

ช่องทางในการรับเงินจากผู้เสียหายคือการโอนเงินผ่านบัญชีธนาคาร บัญชีธนาคารจึงเป็นเครื่องมือที่สำคัญมากของกลุ่มมิจฉาชีพ แต่เพื่อปกปิดตัวตนของกลุ่มมิจฉาชีพ จำเป็นต้องมีการใช้บัญชีที่เจ้าของบัญชีมิใช้ผู้รับเงินหรือมิใช่กลุ่มมิจฉาชีพ บัญชีในลักษณะนี้เรียกว่า “บัญชีม้า” จากการสืบสวนสอบสวนของเจ้าหน้าที่ที่เกี่ยวข้อง พบว่ามีการรับซื้อบัญชีม้าจากบุคคลทั่วไปรวมทั้งมีการจ้างให้เปิดบัญชีเพื่อนำมาใช้ในการหลอกลวงโดยเฉพาะอีกด้วย การได้มาซึ่งบัญชีม้าของมิจฉาชีพนั้น มีทั้งการซื้อขายขาดซึ่งมักซื้อหาในราคาประมาณ ๔๐๐-๑,๐๐๐ บาท โดยเมื่อมีการซื้อขายแล้ว มิจฉาชีพจะนำไปใช้โดยไม่เกี่ยวข้องกับเจ้าของบัญชีตัวจริงแล้ว ยังมีการซื้อขายในลักษณะที่เจ้าของบัญชีทำรายการต่าง ๆ ให้กับมิจฉาชีพด้วย ซึ่งกลุ่มนี้เรียกว่า “ม้าเลี้ยง” โดยม้าเลี้ยงจะได้รับเงินเดือนจากกลุ่มมิจฉาชีพ

ในการเปิดบัญชีม้านั้น ส่วนที่สำคัญอีกประการหนึ่งคือการเปิดระบบการใช้งาน Mobile Banking โดยมิจฉาชีพอาจจะให้มีการใช้ซิมม้าร่วมกับการบัญชีม้า เพื่อนำไปใช้ใน Mobile Banking ได้ อย่างไรก็ดี การใช้งาน Mobile Banking แม้ว่าตอนเริ่มใช้งานจะเป็นกระบวนการที่ต้องทำที่ธนาคาร แต่เมื่อมีการใช้งานตามปกติแล้วไม่ได้มีการตรวจสอบความเป็นตัวตนคู่กันระหว่างเจ้าของบัญชีและเจ้าของเบอร์ จึงเป็นช่องว่างที่มิจฉาชีพจะนำบัญชีม้าและซิมม้าไปใช้ต่อได้

๑.๒.๒ การเข้าถึงเป้าหมาย

เมื่อมีการเตรียมการพร้อมแล้ว มิจฉาชีพก็จะดำเนินการติดต่อหาเป้าหมาย แรกเริ่มนั้น มิจฉาชีพจะสังเกตท่าทีของเป้าหมายว่ามีแนวโน้มที่จะหลงกลหรือไม่ หากเป้าหมายไม่มีท่าทีจะหลงกลได้ มิจฉาชีพจะรีบเปลี่ยนเป้าหมายโดยเร็วที่สุดเพื่อประหยัดเวลา ในปัจจุบัน พบว่ามิจฉาชีพมักเริ่มต้นโดยใช้การโทรด้วยระบบอัตโนมัติ เมื่อเป้าหมายแสดงท่าทีสนใจหรือมีโอกาสที่จะหลงกลแล้ว จึงเป็นการสนทนากับตัวมิจฉาชีพโดยตรง ตัวอย่างเช่น เมื่อมีการใช้ระบบอัตโนมัติโทรไปยังเป้าหมายโดยจัดฉากให้เหมือนเป็นการติดต่อจากหน่วยงานรัฐ และหลอกเป้าหมายว่ามีเป้าหมายมีความเกี่ยวข้องกับอาชญากรรมต่าง ๆ โดยหากเป้าหมายต้องการติดต่อเจ้าหน้าที่หรือทราบรายละเอียดเพิ่มเติม ให้กดเลขหมายบนแป้นในโทรศัพท์ ซึ่งเมื่อเป้าหมายกดเลขตามที่แจ้งแล้ว ก็แสดงว่าเป้าหมายมีความสนใจและมีแนวโน้มที่จะหลงกล มิจฉาชีพจึงจะเข้ามาคุยกับเป้าหมายด้วยตนเอง ซึ่งการใช้ระบบอัตโนมัติเข้ามาช่วยทำให้มิจฉาชีพประหยัดเวลาและทรัพยากรได้มาก เพราะเป็นการกรองเฉพาะเป้าหมายที่มีแนวโน้มจะหลงกลและทำให้การหลอกลวงประสบความสำเร็จได้มากขึ้น จากขั้นตอนนี้ มิจฉาชีพจะเริ่มใช้เทคนิคต่าง ๆ ในการหว่านล้อมเป้าหมายให้มีการโอนเงินให้กับมิจฉาชีพ

๑.๒.๓ การหลอกลวงเป้าหมาย

ในการหลอกลวงเป้าหมายนั้น มิจฉาชีพได้อาศัยเทคนิคหรืออุบายในหลอกลวงที่หลากหลาย มักทำให้เป้าหมายเกิดความรู้สึกบางอย่างที่มากพอจะทำให้เป้าหมายยอมโอนเงินให้กับมิจฉาชีพได้ เช่น ความรู้สึกกลัว ตกใจ อยากได้หรือโลภ เป็นต้น โดยอุบายการหลอกลวงนั้นมีตัวอย่าง ดังนี้

ตารางที่ ๓-๑ ตัวอย่างรูปแบบการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

รูปแบบการใช้กลอุบาย	วิธีการและเทคนิคหลอกลวง
๑. บัญชีเงินฝากถูกอายัดหรือเป็นหนี้บัตรเครดิต	**วิธีการหลอกลวง : แอบอ้างเป็นพนักงานธนาคาร** มิจฉาชีพจะใช้ระบบตอบรับอัตโนมัติแจ้งเป้าหมายว่าจะอายัดบัญชีเงินฝากของเป้าหมาย เนื่องจากเหตุการณ์ต่าง ๆ เช่น เป็นหนี้บัตรเครดิตหรือกระทำการผิดกฎหมาย โดยมีเสียงอัตโนมัติ เช่น “คุณเป็นหนี้บัตรเครดิตกับทางธนาคาร กด 0 เพื่อติดต่อพนักงาน” เมื่อเหยื่อตกใจ ก็จะรีบต่อสายคุยกับมิจฉาชีพทันที หลังจากนั้นมิจฉาชีพจะหลอกถามฐานะทางการเงินของเหยื่อ และหลอกล่อให้โอนเงินมาให้เพื่อตรวจสอบ

ตารางที่ ๓-๑ ตัวอย่างรูปแบบการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

รูปแบบการใช้กลอุบาย	วิธีการและเทคนิคหลอกลวง
๒. บัญชีเงินฝากเกี่ยวข้องกับขบวนการค้ายาเสพติดหรือการฟอกเงิน	**วิธีการหลอกลวง : แอบอ้างเป็นเจ้าหน้าที่ตำรวจ** มิจฉาชีพจะหลอกเป็นเจ้าหน้าที่ตำรวจ โดยเป้าหมายถูกชัดทอดว่าเป็นผู้รับโอนเงินในคดีค้ายาเสพติด หรือคดีฟอกเงิน โดยเป้าหมายต้องโอนเงินไปให้เจ้าหน้าที่เพื่อตรวจสอบ
๓. เงินคืนภาษี	**วิธีการหลอกลวง : แอบอ้างเป็นเจ้าหน้าที่สรรพากร** โดยข้ออ้างคืนเงินภาษีจะถูกใช้ในช่วงที่มีการยื่นภาษีและมีการขอคืนพร้อมกับแจ้งว่า เป้าหมายได้รับภาษีคืนเป็นเงินจำนวนหนึ่ง ซึ่งจะต้องยืนยันรายการและทำตามที่เจ้าหน้าที่บอก แต่ในความเป็นจริงขั้นตอนที่มิจฉาชีพให้เหยื่อทำนั้นเป็นการโอนเงินให้กับมิจฉาชีพ
๔. ได้รับรางวัลจากการจับสลากหรือเสี่ยงโชค	**วิธีการหลอกลวง : แอบอ้างเป็นเจ้าหน้าที่บริษัทหรือตัวแทนองค์กร** มิจฉาชีพจะแจ้งข่าวดีแก่เป้าหมายว่า เป็นผู้โชคดีและได้รับรางวัลใหญ่ หรือเป้าหมายได้รับเงินรางวัลหรือของรางวัลที่มีคุณค่าสูง เมื่อเป้าหมายหลงเชื่อจะหลอกเป้าหมายให้โอนเงินค่าภาษีมูลค่าเพิ่ม หรือค่าธรรมเนียมให้ตามมูลค่าของรางวัล
๕. ข้อมูลส่วนตัวหาย	**วิธีการหลอกลวง : แอบอ้างเป็นเจ้าหน้าที่สถาบันการเงิน** มิจฉาชีพจะเล่าเหตุการณ์ที่ทำให้ข้อมูลของลูกค้าสูญหาย เช่น เหตุการณ์น้ำท่วม จึงขอให้เป้าหมายแจ้งข้อมูลส่วนตัว เช่น วัน/เดือน/ปีเกิด เลขที่บัตรประชาชน เพื่อให้เป็นฐานข้อมูลในการใช้บริการของเป้าหมาย แต่แท้จริงแล้วมิจฉาชีพจะนำข้อมูลเหล่านี้ไปประกอบการปลอมแปลงหรือใช้บริการทางการเงินในนามของเหยื่อ
๖. พัสดุติดด่านศุลกากร	**วิธีการหลอกลวง : แอบอ้างเป็นพนักงานบริษัทขนส่งหรือเจ้าหน้าที่ที่เกี่ยวข้อง** มิจฉาชีพจะโทรมาแจ้งกับเป้าหมายว่ามีพัสดุที่เกี่ยวข้องกับการกระทำผิดกฎหมายส่งมายังที่อยู่ของผู้รับหรือมีการส่งพัสดุจากต่างประเทศ โดยทางบริษัทและเจ้าหน้าที่ของภาครัฐจะขอเข้าไปทำการตรวจสอบและดำเนินคดีตามขั้นตอนกฎหมาย ทำให้ผู้เป้าหมายตกใจกลัวและหลงเชื่อ จึงยินยอมส่งข้อมูลส่วนตัวและโอนเงินไปยังบัญชีที่มิจฉาชีพได้แจ้ง เพื่อให้เจ้าหน้าที่ช่วยเหลือ
๗. เลขหมายโทรศัพท์ถูกระงับการใช้งาน	**วิธีการหลอกลวง : แอบอ้างว่าเป็นเจ้าหน้าที่สำนักงาน กสทช.** มิจฉาชีพจะโทรหาเป้าหมาย อ้างว่าเป็นเจ้าหน้าที่สำนักงาน กสทช. โดยพบว่ามิจฉาชีพมีการอ้างชื่อเจ้าหน้าที่ ซึ่งมิจฉาชีพอาจค้นหาชื่อจากเว็บไซต์ของสำนักงาน กสทช. และแจ้งเป้าหมายว่าเลขหมายของเป้าหมายจะถูกระงับการใช้งาน เนื่องจากได้รับแจ้งความผิดปกติเป็น

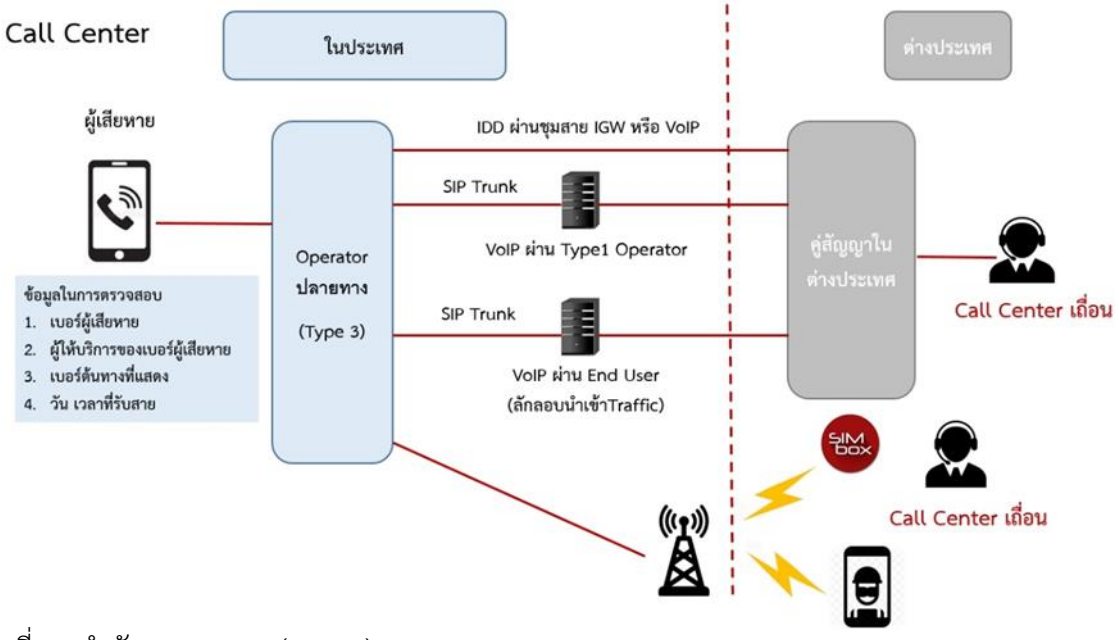
ตารางที่ ๓-๑ ตัวอย่างรูปแบบการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

รูปแบบการใช้กลอุบาย	วิธีการและเทคนิคหลอกลวง
	จำนวนมาก จะตัดสัญญาณโทรศัพท์ในอีก ๒ ชั่วโมง เมื่อเป้าหมายหลงเชื่อ มิจฉาชีพจะขอข้อมูลส่วนตัวรวมทั้งข้อมูลในแอพพลิเคชั่นเช่น ไลน์ และมิจฉาชีพจะส่งลิงก์ที่มีมัลแวร์หรือแฝงการติดตั้งแอพดูดเงินไว้
๘. อ้างว่าเป็นเพื่อนหรือญาติ	**วิธีการหลอกลวง : แอบอ้างว่าเป็นเพื่อนหรือญาติ** มิจฉาชีพจะโทรหาเป้าหมายและทำทีเป็นเพื่อนเก่าหรือญาติ โดยจะให้เป้าหมายลองทายว่าเป็นใคร และใช้ชื่อที่เป้าหมายพูดออกมาเพื่อแอบอ้าง หรือมิจฉาชีพอาจหาข้อมูลจากโซเชียลมีเดียมาก่อนแล้วว่าเพื่อนของเป้าหมายชื่ออะไร จากนั้นจะบอกว่าได้เปลี่ยนเลขหมายโทรศัพท์แล้ว ไม่ให้โทรไปยังเลขหมายเดิมอีก จากนั้นจะเล่าว่ากำลังเดือดร้อนขอยืมเงินเป้าหมาย เมื่อเป้าหมายหลงกลจะขอให้เป้าหมายโอนเงินไปให้

ที่มา : จักรพงษ์ กังวานโสภณ (๒๕๖๕) ประมวลโดยผู้วิจัย

จากการหลอกลวงข้างต้น จะเห็นได้ว่าการหลอกลวงหลายครั้ง มิจฉาชีพได้มีการใช้ข้อมูลส่วนตัวของเป้าหมายเพื่อประกอบการหลอกลวง ทำให้การหลอกลวงมีความแนบเนียนมากขึ้น ซึ่งการได้ไปซึ่งข้อมูลส่วนตัวนั้น ทั้งข้อมูลชื่อ นามสกุล วันเดือนปีเกิด เลขประจำตัวประชาชน ที่อยู่ ก็เป็นอีกปัญหาหนึ่งที่ควรมีการศึกษาและวางมาตรการที่เหมาะสม เนื่องจากเป็นส่วนสำคัญเช่นกันที่ส่งผลกระทบให้ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่แก้ไขได้ยากในปัจจุบัน

แผนภาพที่ ๓-๑ ผังการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่



ที่มา: สำนักงาน กสทช. (๒๕๖๖)

๑.๒.๔ การให้เป้าหมายโอนเงินให้กับมิจฉาชีพ

เมื่อเป้าหมายหลงกลแล้ว ก็จะเข้าสู่ขั้นตอนการโอนเงินไปยังมิจฉาชีพ ซึ่งเมื่อมีการเริ่มสูญเสียทรัพย์สินแล้วก็จะพิจารณาได้ว่าเป้าหมายคือผู้เสียหาย มิจฉาชีพมักนิยมให้มีการโอนเงินผ่าน Mobile Banking เนื่องด้วยปัจจัยที่สำคัญคือความสะดวก รวดเร็วของการทำธุรกรรมต่าง ๆ ลดความเสี่ยงของการไปยังสาขาธนาคาร และผู้กระทำผิดมักพำนักอยู่ในต่างประเทศ การใช้ Mobile Banking จึงมีเหมาะสมที่สุด ในปัจจุบันพบว่ามักไม่มีการให้เป้าหมายโอนเงินผ่านตู้กดเงินอัตโนมัติหรือตู้ ATM แล้ว โดยนอกจากการที่ผู้คนในปัจจุบันหันไปใช้การทำธุรกรรมทางการเงินผ่านระบบ Mobile Banking ซึ่งทำให้เป้าหมายส่วนใหญ่มีการใช้ Mobile Banking เป็นปกติแล้วนั้น ยังพบว่าการทำธุรกรรมผ่านระบบ Mobile Banking จะทำให้เป้าหมายโอนเงินไปถึงบัญชีม้าของมิจฉาชีพในเวลาอันสั้น ในขณะที่เป้าหมายยังไม่สามารถทำความเข้าใจสถานการณ์ได้ หรือยังไม่รู้ตัวว่ากำลังถูกมิจฉาชีพหลอกอยู่ เมื่อเทียบกับการทำธุรกรรมทางการเงินผ่านตู้ ATM ที่เสียเวลาและเป้าหมายอาจจะรู้ตัวว่ากำลังถูกหลอกในระหว่างการเดินทางไปยังตู้ ATM เพราะฉะนั้น การให้โอนเงินผ่าน Mobile Banking จึงมีความนิยมกว่ามาก

เมื่อมีการโอนเงินจากผู้เสียหายมายังบัญชีม้าของมิจฉาชีพแล้ว มิจฉาชีพจะรีบดำเนินการโยกย้ายเงินออกจากบัญชีม้าเล่มแรกไปยังเล่มต่อ ๆ ไป และไปให้ถึงบัญชีสุดท้ายโดยเร็วที่สุด โดยพบว่ามิจฉาชีพจะใช้บัญชีม้าหลายเล่ม เรียกว่าบัญชีม้าแถวที่ ๑ ๒ ๓ ตามลำดับจนถึงบัญชีสุดท้าย การใช้บัญชีม้าเหล่านี้กับเป้าหมายแต่ละคนจะมีการสลับบัญชีม้าที่มีอยู่เพื่อให้เจ้าหน้าที่สามารถติดตามได้ยากขึ้น เมื่อมีการโยกเงินจนถึงบัญชีสุดท้าย จะเป็นการแปลงเงินให้อยู่ในรูปเงินสกุลดิจิทัลหรือ Cryptocurrency หรือโอนออกไปยังกระเป๋าเงินดิจิทัล (Crypto wallet) เพื่อให้เจ้าหน้าที่ไม่สามารถติดตามต่อได้อีก เมื่อเงินได้ไปถึงมิจฉาชีพโดยไม่สามารถติดตามต่อได้ จึงนับว่ากระบวนการการหลอกลวงของมิจฉาชีพสำเร็จแล้ว

๒. การวิเคราะห์พฤติกรรมการกระทำผิดตามหลักการทางจิตวิทยา

จากแนวคิดและหลักการที่มิจฉาชีพใช้ในการหลอกลวงเป้าหมาย พบว่ามีการใช้หลักการการหลอกลวงหลายหลักการ ทว่า จะมีการใช้มากน้อยต่างกันตามแต่สถานการณ์ โดยมีรายละเอียดดังนี้

๒.๑ หลักการเบี่ยงเบนความสนใจ (Distraction Principle) หลักการเบี่ยงเบนความสนใจเป็นหลักการที่สำคัญที่มิจฉาชีพนิยมใช้ ซึ่งจากการพิจารณาพบว่ามิจฉาชีพในกรณีการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ก็มีการใช้การเบี่ยงเบนความสนใจเช่นกัน โดยจุดหลักสำคัญคือการทำให้เป้าหมายพุ่งความสนใจไปที่เรื่องใดเรื่องหนึ่งเป็นอย่างมาก เช่น การหลอกเป้าหมายว่าเป็นผู้โชคดีได้รับรางวัล หรือสิทธิประโยชน์ต่าง ๆ การหลอกเป้าหมายว่ามีพัสดุผิดกฎหมายนำเข้ามาในประเทศ หรือการหลอกลวงว่าเป้าหมายถูกซัดทอดว่าเป็นผู้รับโอนเงินในคดียาเสพติด การหลอกในลักษณะนี้ทำให้เป้าหมายเกิดความดีใจ หวาดกลัวและสนใจแต่จุดนั้น โดยมิได้ให้ความสนใจกับความสมเหตุสมผลอื่น ๆ เช่น อย่างไรก็ดี อาจพิจารณาได้ว่าการที่จะทำให้เป้าหมายเกิดการมุ่งความสนใจไปที่สิ่งหนึ่ง สิ่งนั้นมักมีความเกี่ยวพันกับอารมณ์ ความรู้สึกของเป้าหมายเป็นอย่างมาก เช่น ความรู้สึกหวาดกลัว ความรู้สึกอยากได้หรือโลภ ซึ่งในประเด็นความรู้สึกเหล่านี้ก็เป็นอีกหลักการหนึ่งของการ

หลอกลวงที่ชื่อว่าหลักการความอยากได้อยากมีและความโลภ หรือหลักการตอบสนองตามต้องการพื้นฐานของมนุษย์ซึ่งจะได้มีการอธิบายต่อไป

๒.๒ หลักการการปฏิบัติตามเงื่อนไขในสังคม (Social Compliance Principle) หลักการนี้จัดเป็นอีกหลักการหนึ่งที่สำคัญยิ่งในกรณีการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ โดยตามหลักการแล้ว ผู้คนจะมีความเชื่อในบริบทของสังคมว่าเจ้าหน้าที่รัฐหรือหน่วยงานที่มีชื่อเสียงมีความน่าเชื่อถือ และประชาชนมีหน้าที่ที่จะต้องทำตามอย่างเคร่งครัด ดังนั้น มิจฉาชีพที่โทรเข้ามาหลอกลวงจึงมักปลอมเป็นเจ้าหน้าที่ของหน่วยงานต่าง ๆ เช่น ตำรวจ สำนักงาน กสทช. ธนาคาร ซึ่งการที่ปลอมเป็นเจ้าหน้าที่ในลักษณะนี้ ทำให้ประชาชนยอมทำตามโดยง่าย อย่างไรก็มี มีข้อสังเกตว่าการอ้างเป็นเจ้าหน้าที่ขององค์กรที่มีความน่าเชื่อถือยังเป็นการแสดงถึงอำนาจ (Authority) ที่จะสามารถกระทำการต่าง ๆ ได้ แม้ว่าจะเป็นการกระทำที่ขัดต่อกฎหมายหรือหลักปฏิบัติโดยทั่วไป เช่น การหลอกว่าเป็นตำรวจ แต่สามารถช่วยเป้าหมายที่ถูกหลอกว่าได้เกี่ยวข้องกับคดีอาชญากรรม ให้รอดพ้นจากการถูกดำเนินคดีได้ ซึ่งเป็นการกระทำที่ไม่ถูกต้องตามหลักกฎหมาย หรือมีอำนาจที่จะทำให้เรื่องที่ผิดเป็นถูกได้ จึงอาจพิจารณาได้ว่าการแอบอ้างเป็นเจ้าหน้าที่ของรัฐ นอกจากจะทำให้มีความน่าเชื่อถือ เป้าหมายเชื่อได้โดยง่ายว่าเหตุเกิดขึ้นจริงตามที่มิจฉาชีพหลอกลวง ยังเป็นหลักการที่นำมาใช้เพื่อให้เป้าหมายเกิดความหวาดกลัวในอำนาจของหน่วยงานนั้น ๆ จนสามารถนำไปสู่การโอนเงินให้กับมิจฉาชีพได้

๒.๓ หลักการการคล้อยตามคนหมู่มาก (Herd Principle) หลักการนี้เป็นหลักการที่ไม่นิยมนำมาใช้กับกรณีของการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ เนื่องจากมิจฉาชีพในกลุ่มนี้มักมีการให้เป้าหมายตัดสินใจเองแต่เพียงผู้เดียว และลักษณะการหลอกลวงยังเป็นแบบที่มิจฉาชีพและเป้าหมายไม่ต้องพบหน้ากัน จึงไม่จำเป็นต้องใช้หน้าม้าชี้นำเป้าหมายในกระบวนการหลอกลวง

๒.๔ หลักการความไม่ซื่อสัตย์ (Dishonesty principle) หลักการนี้มักมีการใช้ในการหลอกลวงที่เกี่ยวข้องกับพนันออนไลน์ ซึ่งมักไม่ได้เป็นการโทรไปยังเป้าหมาย แต่ใช้ผ่านช่องทางการสื่อสารด้วยข้อความ เช่น ข้อความสั้นหรือ SMS การใช้แอพพลิเคชั่นในโซเชียลมีเดีย โดยหลอกลวงว่าการันตีผลตอบแทนดี และอาจส่งลิงก์เว็บพนันออนไลน์ที่ฝังมัลแวร์ระบบควบคุมโทรศัพท์ทางไกลไว้ เมื่อเป้าหมายกดเข้าไปในลิงก์ดังกล่าว มิจฉาชีพก็จะควบคุมโทรศัพท์ได้และใช้ Mobile Banking ในโทรศัพท์นั้นโอนเงินเข้าบัญชีม้าของมิจฉาชีพจนหมด หรือเป็นแอพดูดเงินทำการโอนเงินเข้าบัญชีม้าของมิจฉาชีพ เป็นต้น การพนันออนไลน์ในปัจจุบันยังเป็นสิ่งผิดกฎหมาย เพราะฉะนั้น การที่เป้าหมายตัดสินใจเข้าไปเล่นการพนันออนไลน์ ก็นับว่าได้กระทำผิดกฎหมายแล้ว เมื่อเป้าหมายรู้ตัวว่าถูกหลอกก็อาจไม่สามารถดำเนินคดีได้ (กองบัญชีการตำรวจสันติบาล, ๒๕๖๖)

๒.๕ หลักการความใจดี (Kindness Principle) หลักการความใจดีที่พบมากในปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยซึ่งมีลักษณะคล้ายกับกรณีการหลอกลวงที่เกิดขึ้นมากในประเทศสิงคโปร์คือ การหลอกว่าเป็นเพื่อน (Fake friend) โดยมิจฉาชีพจะโทรหาเป้าหมายและทำทีว่าเป็นเพื่อนที่กำลังเดือดร้อน ต้องการความช่วยเหลือ ด้วยการใช้ความใจดีของเป้าหมายที่อยากช่วยเหลือเพื่อนในยามยาก เป้าหมายจึงได้ทำการโอนเงินให้กับมิจฉาชีพ

๒.๖ หลักการความอยากได้อยากมีและความโลภ (Need and Greed Principle) หรือหลักการตอบสนองตามต้องการพื้นฐานของมนุษย์ (Visceral triggers) จากการพิจารณาลักษณะปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ที่เกิดขึ้นในประเทศไทย พบว่าหลักการนี้เป็นหัวใจสำคัญของการหลอกลวงและมีความเกี่ยวพันกับหลักการในข้ออื่น ๆ ของการหลอกลวง เนื่องจากมิจฉาชีพจะมีความเข้าใจในมนุษย์เป็นอย่างดี และมักใช้ความรู้สึกของมนุษย์ซึ่งเป็นจุดอ่อนในการหลอกลวง ทั้งความรู้สึกรัก โลภ กลัว หลง และความต้องการสิ่งเติมเต็มในชีวิตอย่างความรัก จึงอาจกล่าวได้ว่าเป็นหลักการพื้นฐานที่สุดของการหลอกลวงทุกประเภท มิใช่เฉพาะการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เท่านั้น การหลอกโดยใช้ความรักหรือที่เรียกว่า Romance Scam โดยมิจฉาชีพมักเข้าหาเป้าหมายด้วยการใช้สื่ออื่น ๆ ก่อน เช่น โซเชียลมีเดีย และอาจมีการติดต่อผ่านโทรศัพท์เคลื่อนที่ในภายหลังได้ จากนั้นจะพูดคุยกับเป้าหมายจนเป้าหมายหลงรัก และนำไปสู่การโอนเงินให้มิจฉาชีพ การหลอกโดยใช้ความโลภ มักเป็นการหลอกลวงในรูปแบบการหลอกให้ลงทุนหรือเพื่อหารายได้ หลอกว่าเป้าหมายเป็นผู้โชคดีได้รับรางวัล เป็นต้น การหลอกโดยใช้ความกลัว อย่างการโทรมาข่มขู่โดยแอบอ้างว่าเป็นเจ้าหน้าที่ตำรวจ และการหลอกโดยใช้ความหลง อย่างการหลงในการพนัน เป็นต้น ซึ่งความรู้สึกทั้งหมดข้างต้นนี้ เป็นความรู้สึกพื้นฐานที่มนุษย์ทุกคนมีทั้งสิ้น และอาจพิจารณาได้ว่าเป็นจุดที่แก้ไขได้ยาก

๒.๗ หลักการด้านเวลา (Time Principle) ลักษณะเดียวกับกรณีในต่างประเทศ คือ มิจฉาชีพจะหลอกให้เป้าหมายดำเนินการโอนเงินให้เร็วที่สุด เพื่อให้เป้าหมายมีเวลาคิดน้อยที่สุด ซึ่งมักมีการให้โอนผ่าน Mobile Banking เนื่องจากใช้เวลาน้อย จึงกล่าวได้ว่าเป็นผลเสียอีกด้านหนึ่งของ Mobile Application การโอนเงินผ่านโทรศัพท์เป็นวิธีการที่สะดวกและง่ายดายสำหรับผู้ใช้บริการ แต่ในทางหนึ่งก็ทำให้เสียเงินให้กับมิจฉาชีพโดยไม่ทันได้ยั้งคิดได้ง่าย โดยหากเป็นการไปโอนที่ตู้ ATM อาจต้องใช้เวลามากกว่า ซึ่งเป้าหมายอาจจะมีเวลาค่อยคิดทบทวนและไหวตัวทันได้

๒.๘ หลักการสร้างข้อผูกพัน (Commitment) การสร้างข้อผูกพันมักมาในรูปแบบการหลอกลวงแบบหลอกให้ลงทุน โดยมิจฉาชีพจะหลอกให้มีเป้าหมายทดลองลงทุนด้วยเงินจำนวนน้อย ๆ ก่อน และให้ค่าตอบแทนที่สูงกว่าการลงทุนทั่วไปมาก เมื่อเป้าหมายเห็นว่ามีการจ่ายค่าตอบแทนจริง ก็จะลงทุนมากขึ้นเรื่อย ๆ และสุดท้ายมิจฉาชีพก็จะไม่จ่ายค่าตอบแทนให้อีกและยึดเงินดังกล่าวไป อย่างไรก็ดี พบว่าการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มักมีการหลอกลวงในลักษณะนี้ค่อนข้างน้อย เนื่องจากต้องอาศัยช่องทางการสื่อสารอื่น ๆ ประกอบ และต้องใช้เวลามากกว่าจะหลอกลวงได้สำเร็จ

เมื่อพิจารณาถึงหลักการการหลอกลวงทั้ง ๘ ข้อข้างต้น จะเห็นได้ว่าการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยมีการใช้หลักการหลายข้อและเป็นจุดที่แก้ไขได้ยาก เพราะมักเป็นเรื่องของการกระตุ้นอารมณ์ความรู้สึกของเป้าหมาย ซึ่งเป็นจุดอ่อนของมนุษย์ ดังนั้น จึงเป็นการเน้นย้ำถึงจุดประสงค์ในการวางมาตรการที่เหมาะสมว่า การให้ความตระหนักรู้แก่ประชาชนอย่างเดียวนั้นไม่เพียงพอ จะต้องมีมาตรการป้องกันประชาชนจากการเข้าถึงของมิจฉาชีพด้วย

๓. แรงจูงใจของผู้กระทำผิดและผู้เสียหาย

๓.๑ แรงจูงใจของผู้กระทำผิด

โดยทั่วไปแล้ว การหลอกลวงที่เกิดขึ้นมักเป็นการหลอกลวงให้เสียทรัพย์ทั้งสิ้น จึงสามารถกล่าวได้ว่า แรงจูงใจของผู้กระทำผิดประการที่สำคัญที่สุดคือต้องการได้เงิน ซึ่งเงินก็เป็นปัจจัยสำคัญในการดำรงชีวิต จากข้อมูลการให้สัมภาษณ์ พบว่าผู้กระทำผิดที่เข้าร่วมแก๊งคอลเซ็นเตอร์ได้รับค่าตอบแทนสูง โดยจะได้รับเงินเป็นส่วนแบ่งที่คิดตามสัดส่วนของจำนวนเงินที่หลอกได้ อย่างไรก็ดี ได้มีการวิเคราะห์ในมุมต่าง ๆ ของผู้ให้สัมภาษณ์เช่นกันว่า การเข้าไปร่วมขบวนการหลอกลวงได้นั้น แต่ละคนอาจมีเหตุผลความจำเป็นเพื่อเอาชีวิตรอด หรืออาจเป็นทางเลือกสุดท้ายในชีวิต ซึ่งก็อาจสะท้อนถึงปัญหาเศรษฐกิจและสังคมในไทยได้ด้วยเช่นกัน ประกอบกับปัจจัยแวดล้อมด้วยลักษณะการกระทำความผิดที่ไม่สามารถจับกุมได้ง่าย ไม่เห็นผลของการกระทำผิดที่ชัดเจนเหมือนกับการปล้นทองแล้วมีคนวิ่งไล่ตาม ด้วยข้อจำกัดของกฎหมายที่ไม่สามารถบังคับใช้นอกราชอาณาจักรไทยได้ นอกจากนี้ ยังมีข้อมูลส่วนหนึ่งได้ระบุถึงผู้กระทำผิดที่ถูกจับกุมได้มีมักการกล่าวอ้างว่า ถูกหลอกไปทำงาน โดยหากไม่ทำงานตามที่ได้รับสั่ง จะถูกทำร้ายร่างกายรวมถึงการกักขังหน่วงเหนี่ยว ซึ่งในประเด็นนี้นั้น อาจต้องมีข้อมูลสนับสนุนเพิ่มเติม เนื่องจากการจับกุมในปัจจุบันยังมีจำนวนน้อย จึงอาจยังไม่สามารถสรุปได้

๓.๒ แรงจูงใจของผู้เสียหาย

กลุ่มผู้เสียหายสามารถกล่าวโดยสรุปได้ว่าเป็นกลุ่มที่ “ขาด” เหตุปัจจัยบางประการไป ทำให้ตกเป็นผู้เสียหาย เช่น การขาดความรัก ขาดเงิน ขาดความรู้เท่าทัน เป็นต้น นอกจากนี้ เมื่อใช้ทฤษฎีข้อผิดพลาดในการตัดสินใจ (Error in judgement) นั้น ก็พบว่านอกจากการขาดปัจจัยในชีวิตทำให้ผู้เสียหายหลงกลมิจฉาชีพแล้ว ผู้เสียหายยังถูกโจมตีจุดอ่อนซึ่งส่งผลต่อการตัดสินใจได้ เช่น ผู้เสียหายบางกลุ่มเป็นแพทย์ เจ้าของธุรกิจ ข้าราชการ ซึ่งในการรับรู้ของบุคคลทั่วไปกล่าวได้ว่าเป็นผู้มีความรู้ แต่ก็สามารถหลงกลผู้กระทำผิดได้ เนื่องจากถูกหลอกลวงโดยอาศัยจุดอ่อนในการตัดสินใจของผู้เสียหาย ซึ่งมักมีอารมณ์ความรู้สึกหรือภูมิหลัง (Background) มาเกี่ยวข้อง และจุดอ่อนเหล่านี้ไม่ได้เกี่ยวข้องโดยตรงกับความรู้ความสามารถ นอกจากนี้ ยังมีการกล่าวถึงลักษณะนิสัยบางประการของผู้เสียหายเองด้วย เช่น นิสัยขี้กลัว เมื่อถูกข่มขู่ก็ยอมทำตามคำสั่งโดยไม่ขัดขืน นิสัยโลภอยากได้เงินแต่ไม่อยากทำงานหนัก จึงตกเป็นผู้เสียหายในการหลอกที่ลวงว่าจะให้เงินรางวัลเป็นจำนวนมาก หรือการหลอกลวงที่เกี่ยวข้องกับการพนันออนไลน์ เป็นต้น อย่างไรก็ดี มีข้อสังเกตว่าการที่เป้าหมายถูกหลอกว่ามีความเกี่ยวข้องกับสิ่งผิดกฎหมาย และเป้าหมายก็เชื่อโดยง่าย มีความเป็นไปได้เช่นกันว่าเป้าหมายรายนั้นก็มีความเกี่ยวข้องกับสิ่งผิดกฎหมายอยู่เดิม จึงเชื่อได้สนิทใจเมื่อได้รับสายจากมิจฉาชีพ ซึ่งในประเด็นนี้จำเป็นต้องใช้ข้อมูลจากผู้เสียหาย และอาจมีการพิจารณาในประเด็นนี้เพิ่มเติมในงานวิจัยอื่น ๆ ต่อไป

ผลกระทบที่เกิดขึ้นจากการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ต่อสังคมและผู้บริโภค

๑. ผลกระทบต่อประชาชน

๑.๑ การสูญเสียทรัพย์สิน ซึ่งมีมูลค่าความเสียหายมาก

การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สร้างผลกระทบประการที่สำคัญคือการที่ประชาชนจำนวนมากถูกหลอกและเสียทรัพย์สินให้กับมิจฉาชีพ โดยมีรายงานว่าบางรายเสียเงินเก็บทั้งหมดที่มี นำไปสู่ปัญหาสุขภาพจิตและการฆ่าตัวตาย จึงกล่าวได้ว่ามีผลกระทบต่อทั้งในแง่ทรัพย์สินและชีวิตของผู้เสียหายได้

๑.๒ การพลาดรับสายโทรศัพท์ในเรื่องจำเป็นเร่งด่วน

เมื่อประชาชนได้รับข่าวสารรายงานการหลอกลวงมากขึ้น ประชาชนจำนวนมาก็จะเกิดความระแวงว่าสายเรียกเข้าที่ตนได้รับนั้นเป็นมิจฉาชีพหรือไม่ ทำให้หลายคนเลือกที่จะไม่รับสายที่ไม่รู้จัก หรือการใช้แอพพลิเคชั่น การใช้บริการที่ตัดสายที่ต้องสงสัยว่าเป็นมิจฉาชีพออกไปตั้งแต่ต้น ซึ่งสายเรียกเข้าเหล่านั้นรวมถึงสายเรียกเข้าที่มีความสำคัญเร่งด่วนจากญาติ ครอบครัว เพื่อน และทำให้พลาดการแจ้งข่าวที่สำคัญไปด้วย เช่น การที่ใช้การตัดสายที่มี Prefix +๖๙๗ +๖๙๘ ออกไป ทำให้ไม่ได้รับสายอุบัติเหตุเร่งด่วนของญาติในต่างประเทศ เป็นต้น

๑.๓ การพลาดโอกาสในการได้รับข้อเสนอที่ดี

นอกจากสายเรียกเข้าจากคนสำคัญแล้ว ประชาชนจำนวนมากยังพลาดโอกาสได้รับข้อเสนอที่ดีจากผู้ประกอบการด้วย ซึ่งบ่อยครั้งที่ผู้ประกอบการจะติดต่อลูกค้าเพื่อเสนอเงื่อนไขหรือโปรโมชั่นต่างๆ ทางโทรศัพท์ เมื่อผู้รับได้ตัดสายเหล่านั้นทิ้งไปแล้ว ก็นับได้ว่าพลาดสิทธิประโยชน์ที่ดีไป

๑.๔ ผลกระทบต่อสุขภาพจิต

ประชาชนทั้งกลุ่มที่เป็นผู้เสียหายก็จะเกิดความทุกข์จากการสูญเสียทรัพย์สินดังที่ได้มีการกล่าวข้างต้นว่าผู้เสียหายบางรายตัดสินใจฆ่าตัวตาย ซึ่งเป็นความเสียหายที่ประเมินเป็นตัวเลขไม่ได้ และอาจพิจารณาได้ว่าสร้างความเสียหายไปยังครอบครัวและคนรอบข้างของผู้เสียหายเองด้วย นอกจากนี้ ประชาชนที่รับรู้ข่าวสารก็จะเกิดความรู้สึกวิตกกังวล หวาดระแวง และเกิดความไม่สบายใจเมื่อมีสายเรียกเข้าอีกด้วย

๒. ผลกระทบต่อหน่วยงานที่เกี่ยวข้อง

๒.๑ เกิดภาพลักษณ์ที่ไม่ดีต่อประชาชน

เนื่องจากมิจฉาชีพมักนำชื่อหน่วยงานต่าง ๆ ไปแอบอ้าง โดยเฉพาะหน่วยงานรัฐที่เป็นที่รู้จักและมีความน่าเชื่อถือ จึงทำให้หน่วยงานนั้นเสียภาพลักษณ์ที่ดีไป ทั้งจากการที่ถูกนำไปแอบอ้างและมีประชาชนบางส่วนหลงเชื่อ และทั้งเมื่อเกิดปัญหาขึ้น ประชาชนจำนวนมากก็จะคาดหวังให้หน่วยงานต่าง ๆ รับผิดชอบกับปัญหาโดยการเข้ามาแก้ไขปัญหาให้หมดไป ซึ่งหน่วยงานเหล่านั้นเป็นได้ทั้งหน่วยงานที่ถูกมิจฉาชีพแอบอ้างและมิได้ถูกแอบอ้างแต่ประชาชนเห็นว่ามีความเกี่ยวข้องกับปัญหา ด้วยข้อจำกัดของอำนาจหน้าที่ของแต่ละหน่วยงาน อาจทำให้ไม่สามารถแก้ปัญหา

การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ได้ทั้งหมด ประชาชนที่ไม่เข้าใจในเรื่องข้อจำกัดก็จะเกิดการกล่าวโทษได้ว่าหน่วยงานนั้นว่าขาดความรับผิดชอบ

๒.๒ เสียทรัพยากรสำหรับการเตรียมระบบป้องกันมิจฉาชีพ

หน่วยงานที่เกี่ยวข้องจำเป็นต้องจัดเตรียมมาตรการในการรับมือกับปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ทั้งภาครัฐและเอกชน ซึ่งทำให้สูญเสียทั้งทรัพยากร งบประมาณ และเวลา เช่น ผู้ประกอบการในกิจการโทรคมนาคมจะต้องเตรียมระบบป้องกันมิจฉาชีพให้กับผู้ใช้บริการของตนเอง โดยในปัจจุบันพบว่ามีการจัดทำช่องทางให้ผู้ใช้บริการรายงานหรือร้องเรียนเมื่อได้รับสายจากมิจฉาชีพ รวมทั้งยังต้องมีการจ้างบุคลากรเพื่อเข้ามาดูแลระบบ และทำหน้าที่รับเรื่องร้องเรียนจากผู้ใช้บริการ เป็นต้น

๓. ผลกระทบต่อสังคม

จากปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ที่เพิ่มมากขึ้น ทำให้ประชาชนที่รับรู้ข่าวสารอยู่ในภาวะวิตกกังวล และเกิดเป็นความหวาดระแวงต่อกันได้

๔. ผลกระทบต่อประเทศ

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สามารถกล่าวได้ว่ามีผลกระทบต่อเศรษฐกิจของประเทศ เนื่องจากผู้เสียหายจะมีการโอนเงินให้กับมิจฉาชีพ และมิจฉาชีพจะถ่ายเททรัพย์สินออกนอกประเทศในที่สุด โดยพบว่านายทุนหรือหัวหน้าขบวนการมักเป็นชาวต่างชาติ นอกจากนี้ยังพบว่าเมื่อประชาชนจำนวนถูกหลอกและเสียทรัพย์สินไปแล้ว ก็จะขาดความสามารถในการใช้จ่ายเพื่อขับเคลื่อนเศรษฐกิจภาพรวมของประเทศอีกด้วย

มาตรการและข้อกฎหมายต่าง ๆ ที่เกี่ยวข้องในการแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

ปัจจุบัน กฎหมายที่บังคับใช้เพื่อป้องกันและปราบปรามผู้กระทำผิดฐานความผิดหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ฉบับสำคัญคือ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ลงวันที่ ๑๖ มีนาคม ๒๕๖๖ (พ.ร.ก. อาชญากรรมทางเทคโนโลยี) โดย พ.ร.ก. ฉบับนี้เป็นกฎหมายฉบับล่าสุดที่บัญญัติขึ้นเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีรวมทั้งการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ด้วย โดยในหมายเหตุของ พ.ร.ก. อาชญากรรมทางเทคโนโลยีได้กล่าวถึงเหตุผลของการประกาศใช้ไว้ดังนี้

> “เหตุผลในการประกาศใช้พระราชกำหนดฉบับนี้ คือ โดยที่ปัจจุบันมีการใช้วิธีการทางเทคโนโลยีหลอกลวงประชาชนทั่วไปผ่านอุปกรณ์เทคโนโลยีต่าง ๆ จนทำให้ประชาชนสูญเสียทรัพย์สินเป็นจำนวนมาก และผู้หลอกลวงได้โอนทรัพย์สินที่ได้จากการกระทำความผิดดังกล่าวนั้นผ่านบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลอื่นต่อไปเป็นทอด ๆ อย่างรวดเร็ว เพื่อปกปิดหรืออำพรางการกระทำความผิด ซึ่งแต่ละวันประชาชนผู้สุจริตถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมาก และการหลอกลวงดังกล่าว ซึ่งเป็นการกระทำความผิดได้เพิ่มมากขึ้น ส่งผลกระทบต่อประชาชนในวงกว้างและเป็นอันตรายร้ายแรงต่อระบบเศรษฐกิจของประเทศ เป็นกรณีฉุกเฉินที่มีความ

จำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้ เพื่อประโยชน์ในอันที่จะต้องมีมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีดังกล่าว เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ จึงจำเป็นต้องตราพระราชกำหนดนี้”

พ.ร.ก. ฉบับนี้เป็นการประกาศใช้เพื่อแก้ไขข้อจำกัดของกฎหมายเดิมที่มีอยู่ซึ่งนำมาใช้กับปัญหาอาชญากรรมออนไลน์ได้อย่างไม่มีประสิทธิภาพเท่าที่ควร เนื่องจากการเปลี่ยนแปลงไปอย่างรวดเร็วของลักษณะของอาชญากรรม โดย พ.ร.ก. ฉบับนี้มีการกำหนดที่สำคัญ ดังนี้

๑. กำหนดหน่วยงานรับผิดชอบ

ใน พ.ร.ก. อาชญากรรมทางเทคโนโลยีได้มีการกำหนดอย่างชัดเจนถึงหน่วยงานที่มีหน้าที่รับผิดชอบต่อกรณีอาชญากรรมทางเทคโนโลยี ซึ่งได้แก่ สำนักงานตำรวจแห่งชาติ สถาบันทางการเงินซึ่งหมายถึงธนาคารพาณิชย์และสถาบันทางการเงินของรัฐ ผู้ประกอบธุรกิจตามกฎหมายว่าด้วยการชำระเงิน กระทรวงดิจิทัลเพื่อเศรษฐกิจสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน ธนาคารแห่งประเทศไทย สำนักงาน กสทช. และผู้ให้บริการเครือข่ายโทรศัพท์และบริการโทรคมนาคมอื่น

๒. กำหนดให้มีการเปิดเผยข้อมูลที่เป็นประโยชน์ต่อการสืบสวนสอบสวน

หน่วยงานที่ถูกกำหนดใน พ.ร.ก. อาชญากรรมทางเทคโนโลยี ในมาตรา ๔ และ ๕ มีหน้าที่ต้องให้ความร่วมมือในการเปิดเผยหรือแลกเปลี่ยนข้อมูลแก่สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน เช่น ข้อมูลการลงทะเบียนผู้ใช้งานหรือข้อมูลจราจรทางคอมพิวเตอร์ เมื่อมีการแจ้งความร้องทุกข์ หน่วยงานที่ทำหน้าสืบสวนสอบสวนเหล่านี้มีอำนาจนำข้อมูลไปใช้ประโยชน์เพื่อป้องกัน ปราบปราม หรือระงับอาชญากรรมทางเทคโนโลยีได้

๓. กำหนดให้มีการแจ้งความร้องทุกข์ที่ใดก็ได้ในราชอาณาจักรไทย

แต่เดิมนั้น มีการถกเถียงในเรื่องของสถานที่เกิดเหตุของคดีอาชญากรรมทางเทคโนโลยีว่าควรเป็นที่ใด เช่น ควรเป็นสถานที่ที่ผู้เสียหายถูกหลอกลวง หรือสถานที่ที่มีการโอนทรัพย์สินไปให้มิจฉาชีพ ด้วยลักษณะของอาชญากรรมทางเทคโนโลยีรวมทั้งการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ไม่มีสถานที่เกิดเหตุเฉพาะเจาะจง ใน พ.ร.ก. อาชญากรรมทางเทคโนโลยีจึงกำหนดในมาตรา ๘ ให้สามารถร้องทุกข์ที่ใดก็ได้ในราชอาณาจักร และสามารถร้องทุกข์ได้ทั้ง ณ สถานีตำรวจ กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี หรือร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ก็ได้

๔. กำหนดให้มีการระงับธุรกรรมทางการเงินทุกทอดไว้ทันที

เพื่อให้สามารถระงับความเสียหายและเพื่อการสอบสวน พ.ร.ก. อาชญากรรมทางเทคโนโลยีได้กำหนดในมาตรา ๖ และ ๗ ให้สถาบันทางการเงินและผู้ประกอบธุรกิจระงับการทำธุรกรรมที่สงสัยว่าเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีหรือการกระทำความผิดมูลฐานหรือความผิดฐานฟอกเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน โดยการระงับธุรกรรมนั้นจะต้องระงับไว้ทันทีเป็นการชั่วคราวไว้ไม่เกินเจ็ดวันนับแต่มีเหตุสงสัย นอกจากการระงับธุรกรรมที่ต้องสงสัยแล้ว ยังต้องเป็นการระงับธุรกรรมทุกทอดที่เกี่ยวข้อง นอกจากนี้ หากมีผู้เสียหาย

แจ้งความร้องทุกข์แก่พนักงานสอบสวน ให้สถาบันทางการเงินและผู้ประกอบธุรกิจระงับธุรกรรมทุกทอดที่เกี่ยวข้องไว้เจ็ดสิบสองชั่วโมง และพนักงานสอบสวนต้องดำเนินการพิจารณาต่อไปในเวลาไม่เกินเจ็ดวัน

๕. กำหนดโทษของเจ้าของบัญชีม้าและซิมม้า

เนื่องจากบัญชีม้าและซิมม้าเป็นเครื่องมือที่สำคัญของมิจฉาชีพในการประกอบอาชญากรรม และยังมีประชาชนจำนวนหนึ่งที่ไม่ระวังการเปิดบัญชีม้าหรือซิมม้า และให้มีการซื้อขายบัญชีม้าและซิมม้าได้ ทำให้ปัญหาอาชญากรรมทางเทคโนโลยีไม่สามารถกำจัดได้ง่าย พ.ร.ก. อาชญากรรมทางเทคโนโลยี มาตรา ๙ ๑๐ และ ๑๑ จึงได้กำหนดโทษแก่ผู้ที่เปิดบัญชีม้าและซิมม้า รวมทั้งผู้ที่เป็นธุระจัดหา โฆษณา ซื้อขายหรือเป็นคนกลางในการซื้อขาย จะต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท

นอกจาก พ.ร.ก. อาชญากรรมทางเทคโนโลยี แล้ว กฎหมายฉบับอื่นนั้นก็ยังมีผลบังคับใช้เช่นกัน ซึ่งได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ โดยกฎหมายนี้ก็สามารถพิจารณาได้ว่าเป็นส่วนเสริม พ.ร.ก. อาชญากรรมทางเทคโนโลยี เช่น พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ ได้กำหนดให้มีการระงับบัญชีเงินฝากของผู้ต้องสงสัยว่ามีความเกี่ยวข้องกับการฟอกเงินในทุกบัญชีที่ผู้ต้องสงสัยคนนั้นครอบครอง มิใช่เฉพาะบัญชีที่มีธุรกรรมน่าสงสัยเท่านั้น กฎหมายฉบับนี้จึงสามารถนำมาใช้เสริมกับ พ.ร.ก. อาชญากรรมทางเทคโนโลยี โดยเมื่อมีการระงับบัญชีที่มีธุรกรรมอันต้องสงสัยว่าเกี่ยวข้องกับอาชญากรรมออนไลน์ตาม พ.ร.ก. อาชญากรรมทางเทคโนโลยีแล้ว ก็จะสามารถใช้พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ เสริมในการระงับบัญชีทุกบัญชีของผู้ต้องสงสัยได้ เนื่องจากอาจพิจารณาได้ว่าเจ้าของบัญชีนั้นอาจเปิดบัญชีอื่น ๆ อีกหลายเล่มเพื่อใช้ในการหลอกลวง

ทั้งนี้ กฎหมายที่ได้มีการอธิบายข้างต้นเป็นกฎหมายที่นำมาใช้ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยเมื่อมีการจับกุมผู้กระทำผิดแล้ว ก็จะต้องมีการพิจารณาประมวลกฎหมายอาญา เนื่องจากการหลอกลวงเป็นความผิดฐานฉ้อโกง ซึ่งความผิดฐานฉ้อโกงประชาชนนั้นเข้าความผิดตามที่กำหนดไว้ในประมวลกฎหมายอาญา เช่น มาตรา ๓๔๑ ๓๔๒ และ ๓๔๓ เป็นต้น

การดำเนินมาตรการของสำนักงาน กสทช. และหน่วยงานที่เกี่ยวข้อง

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นปัญหาที่มีความเกี่ยวข้องกับหลายหน่วยงานทั้งภาครัฐและเอกชน จึงมีหลายหน่วยงานที่เข้ามาแก้ปัญหาดังกล่าวในปัจจุบัน ทั้งหน่วยงานที่รับผิดชอบในเรื่องการจับกุมผู้กระทำผิดอย่างสำนักงานตำรวจแห่งชาติ และ บช. สอท. ก็ได้มีบทบาทอย่างมากในการแก้ปัญหา เช่น การจัดทำช่องทางในการแจ้งความร้องทุกข์ออนไลน์ผ่านเว็บไซต์ thaipoliceonline.com การผลักดันในเกิดการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ซึ่งเป็นกฎหมายที่แก้ไขจุดบกพร่องของการใช้กฎหมายเดิม อีกทั้งหน่วยงานเอกชนก็เข้ามามีบทบาทในการแก้ไขปัญหามากขึ้น เช่น การจัดตั้งศูนย์

รับเรื่องร้องเรียนจากผู้ใช้บริการ และมีการดำเนินการประสานงานกับหน่วยงานอื่นที่เกี่ยวข้อง ทั้งนี้ หน่วยงานรัฐที่สำคัญอีก ๒ หน่วยงาน ได้แก่ สำนักงาน กสทช. และ ธนาคารแห่งประเทศไทย (ธปท.) ในฐานะหน่วยงานที่มีส่วนสำคัญกับเครื่องมือของมิจฉาชีพอย่างซิมม้าและบัญชีม้า ก็เป็นหน่วยงานที่มีมาตรการอย่างเข้มแข็ง ดังนี้

๑. สำนักงาน กสทช.

สำนักงาน กสทช. ได้รับการร้องเรียนจากผู้ใช้บริการโทรศัพท์เคลื่อนที่กรณีมีมิจฉาชีพส่งข้อความสั้น (SMS) หลอกลวงผู้ใช้บริการโทรศัพท์เคลื่อนที่ในรูปแบบต่าง ๆ และกรณีการฉ้อโกงประชาชนโดยแสดงตนเป็นบุคคลอื่นผ่านระบบโทรศัพท์และสื่ออิเล็กทรอนิกส์ สำนักงาน กสทช. จึงได้กำหนดมาตรการและแนวทางการแก้ไขปัญหาดังกล่าวเพื่อกำหนดบทบาทหน้าที่ความรับผิดชอบของผู้รับใบอนุญาตที่เกี่ยวข้องกับกรณีดังกล่าวให้ชัดเจนและเพื่อป้องกันแก้ไขปัญหาความเดือดร้อนให้กับประชาชนได้ทันต่อสถานการณ์

๑.๑ การจัดตั้งคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งโทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง

เพื่อให้การดำเนินการแก้ไขปัญหาแก๊งโทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง เกิดการบูรณาการการทำงานระหว่างหน่วยงานที่เกี่ยวข้องเป็นไปด้วยความเรียบร้อย รวดเร็ว และมีประสิทธิภาพ นำไปสู่การปฏิบัติอย่างเป็นรูปธรรม กสทช. จึงได้มีมติให้สำนักงาน กสทช. แต่งตั้งคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งโทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง (คณะทำงานพหุภาคีฯ) เพื่อศึกษา วิเคราะห์ มาตรการและข้อกฎหมายต่าง ๆ ที่เกี่ยวข้องในการแก้ไขปัญหาแก๊งโทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง สร้างช่องทางเพื่อรับแจ้งปัญหาระหว่างหน่วยงาน และออกแบบกระบวนการในการป้องกันและจัดการปัญหา SCAM ประกอบด้วยผู้แทนหน่วยงานต่าง ๆ ที่เกี่ยวข้อง ได้แก่ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ธนาคารแห่งประเทศไทย กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ สภาองค์กรของผู้บริโภค และผู้ให้บริการโทรศัพท์เคลื่อนที่

๑.๒ การแก้ไขปัญหามิจฉาชีพส่งข้อความสั้น (SMS) หลอกลวงประชาชน

ปัจจุบัน มิจฉาชีพได้ส่ง SMS หลอกลวงประชาชน ในรูปแบบต่าง ๆ อาทิ การแจ้งเตือนระบบธุรกรรมการเงินอิเล็กทรอนิกส์ (E-Banking) หรือการแจ้งเกี่ยวกับการทำธุรกรรมการเงินต่าง ๆ หรือข้อความเชิญชวนเล่นการพนัน/เข้าเว็บอนาจารล่วงละเมิดทางเพศ โดยผู้ใช้บริการที่ไม่ระมัดระวังหรือรู้ไม่เท่าทัน อาจกดลิงค์ที่แนบมา หรือกรอกข้อมูลส่วนบุคคล ทั้งชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ซึ่งอาจทำให้ข้อมูลส่วนบุคคล ข้อมูลธุรกรรมทางการเงิน หรือข้อมูลสำคัญอื่น ๆ เช่น เลขบัตรประจำตัวประชาชน รหัสผ่านที่ใช้ครั้งเดียว (One Time Password : OTP) รั่วไหล หรือถูกนำไปใช้ในการกระทำความผิด

สำนักงาน กสทช. ได้ดำเนินการแก้ไขปัญหา โดยจัดทำระบบฐานข้อมูล Sender Name เพื่อให้ผู้ให้บริการสามารถตรวจสอบความซ้ำซ้อน Sender Name และเพื่อให้สำนักงาน กสทช. ใช้เป็นข้อมูลในการกำกับดูแล รวมถึงจัดทำแนวปฏิบัติการกำกับดูแลการให้บริการ

ส่งข้อความสั้น (SMS) เพื่อเป็นแนวทางกำกับดูแลการให้บริการส่งข้อความสั้นกับผู้รับใบอนุญาตประกอบกิจการโทรคมนาคม

๑.๓ การแก้ไขปัญหาการฉ้อโกงประชาชนโดยแสดงตนเป็นบุคคลอื่นผ่านระบบโทรศัพท์และสื่ออิเล็กทรอนิกส์ (แก๊ง Call Center)

ในช่วงแรก มิจฉาชีพใช้วิธีการการโทรจากต่างประเทศโดยใช้เครือข่ายอินเทอร์เน็ตผ่านเทคโนโลยี Voice over Internet Protocol (VoIP) ปลอมเลขหมายเป็นเลขหมายโทรศัพท์ประจำที่ เลขหมายโทรศัพท์แบบสั้น ๔ หลักของหน่วยงานภาครัฐ เช่น ตำรวจ ศาล หรือสำนักงาน กสทช. เพื่อข่มขู่ประชาชนให้เกิดความกลัว และหลอกให้โอนเงิน หรือปลอมเป็นหน่วยงานเอกชน เช่น บริษัทส่งของ เพื่อหลอกว่ามีพัสดุมาส่งต้องชำระเงิน ธนาคาร เพื่อหลอกว่ามียอดค้างชำระบัตรเครดิตต้องโอนมาชำระด่วน โดยรูปแบบการโทรหลอกลวงของแก๊ง Call Center แบ่งเป็น ๒ วิธี ได้แก่

การโทรจากต่างประเทศ มี ๒ รูปแบบ ดังนี้

๑) การโทรจากต่างประเทศโดยใช้เครือข่ายอินเทอร์เน็ตผ่านเทคโนโลยี Voice over Internet Protocol (VoIP) ซึ่งเป็นกรณีที่ทราฟฟิกการโทรที่เข้ามาจากต่างประเทศไม่มีการกำหนดเลขหมายต้นทาง (Non Calling Line Identification)

๒) การโทรจากต่างประเทศผ่านผู้ให้บริการโทรศัพท์ระหว่างประเทศ (IDD) โดยผู้ให้บริการต้นทางจะเติม Country Code หน้าหมายเลขต้นทางซึ่งสามารถระบุประเทศต้นทางได้ (Calling Line Identification) โดยผู้ให้บริการในประเทศไทยจะไม่มีการแปลงหมายเลขก่อนส่งไปยังหมายเลขปลายทาง

<u>การดำเนินการแก้ไขปัญหา</u>

๑) ระงับทราฟฟิคการโทรเข้าจากต่างประเทศมายังเลขหมายปลายทางของประเทศไทยซึ่งมีรูปแบบของเลขหมายที่โทรเข้าเป็น “เลขหมายสำหรับโทรศัพท์ประจำที่” “เลขหมายโทรศัพท์แบบสั้น” และ “เลขหมายที่มีเลขหมายนำกลุ่ม ๔ หลัก” ของประเทศไทย

๒) ระงับทราฟฟิคการโทรเข้าจากต่างประเทศมายังเลขหมายปลายทางของประเทศไทย ซึ่งมีรูปแบบของเลขหมายที่โทรเข้าเป็นรหัสโทรศัพท์ประจำประเทศ (Country Code) ที่ยังไม่ได้กำหนดโดย ITU

๓) ในกรณีทราฟฟิคการโทรเข้าที่มาจากต่างประเทศไม่มีการกำหนดเลขหมายต้นทาง (Non Calling Line Identification : Non CLI) ซึ่งมาจากช่องทาง VoIP ให้ดำเนินการเพิ่ม Prefix โดยใช้เครื่องหมาย “+๖๙๗” นำหน้าเลขหมายที่โทรเข้า เพื่อให้ประชาชนทราบว่าเป็นการโทรเข้าจากต่างประเทศ

๔) กำหนดให้ผู้ให้บริการโทรศัพท์ระหว่างประเทศ ผู้ให้บริการ Call Termination และผู้ให้บริการโทรศัพท์เคลื่อนที่จะต้องเพิ่ม Prefix สำหรับกรณีบริการที่ระบุเลขหมายต้นทางจากต่างประเทศ (Calling Line Identification: CLI) โดยใช้เครื่องหมาย “+๖๙๘” นำหน้าเลขหมายที่เป็น Roaming จากต่างประเทศ (สำหรับทราฟฟิกที่มาจากประเทศที่ใช้งาน Country Code ตามที่สหภาพโทรคมนาคมระหว่างประเทศ (ITU) กำหนด มีการแสดงเครื่องหมาย “+” Prefix ของประเทศนั้น ๆ อยู่แล้ว)

๕) จัดทำบริการ USSD (Unstructured Supplementary Services Data) หมายเลข *๑๓๘ เพื่อให้ผู้ใช้บริการสามารถเลือกปฏิเสธการรับสายที่เป็นทราฟฟิกจากต่างประเทศได้ ทั้งนี้ต้องมีระบบให้ผู้ใช้บริการสามารถยกเลิกความประสงค์ดังกล่าวได้

การโทรจากในประเทศ

มิจฉาชีพมักใช้วิธีการซื้อซิมเป็นจำนวนมากเพื่อนำไปใช้โทรศัพท์หลอกลวงประชาชน กสทช. จึงได้มีมาตรการแก้ไขปัญหาและจัดระเบียบการลงทะเบียนซิมเพิ่มเติม

<u>การดำเนินการแก้ไขปัญหา</u>

๑) กำหนดให้ผู้ให้บริการทุกรายต้องควบคุมจำนวนการลงทะเบียนผู้ใช้บริการขอตนเองในกรณีบุคคลธรรมดา ให้มีจำนวนไม่เกิน ๕ เลขหมายต่อหนึ่งผู้ใช้บริการ ทั้งนี้ หากผู้ใช้บริการมีความประสงค์ที่จะลงทะเบียนมากกว่า ๕ เลขหมาย จะต้องดำเนินการลงทะเบียน ณ ศูนย์ให้บริการของผู้ให้บริการเท่านั้น

๒) จัดทำมาตรการเชิงรุกโดยดำเนินการติดตามตรวจสอบทราฟฟิกการโทรเข้าจากต่างประเทศที่มีพฤติกรรมการใช้งานที่ผิดปกติและมีแนวโน้มการใช้งานที่อาจเข้าข่ายเป็นการกระทำผิดกฎหมาย เมื่อได้ตำแหน่งพื้นที่ที่กระทำความผิดที่ชัดเจนแล้ว ผู้ให้บริการจะแจ้งข้อมูลไปยังสำนักงานตำรวจแห่งชาติ เพื่อดำเนินการทางกฎหมายต่อไป

๑.๔ การสร้างความความตระหนักรู้

โลกในปัจจุบันเทคโนโลยีมีการเปลี่ยนแปลงที่รวดเร็ว เช่นเดียวกันกับรูปแบบการหลอกลวงที่ปรับเปลี่ยนไปอย่างรวดเร็ว การป้องกันที่ดีที่สุดคือการสร้างภูมิคุ้มกันให้กับประชาชน ซึ่งเป็นการเสริมแรงให้ประชาชนผ่านข้อมูลที่ทันสมัย เป็นปัจจุบันเกี่ยวกับรูปแบบกลโกงต่าง ๆ เพื่อสร้างการรู้เท่าทันอย่างมีประสิทธิภาพ

สำนักงาน กสทช. ได้ดำเนินการเพื่อสร้างความตระหนักรู้ให้กับประชาชนโดยจัดทำฐานข้อมูลชื่อ “SCAM Alert/เท่าทันมิจฉาชีพ” เป็นการรวบรวมตัวอย่างการฉ้อโกงผ่านระบบโทรศัพท์ เคลื่อนที่และสื่ออิเล็กทรอนิกส์ วิธีการแก้ไขปัญหาเฉพาะหน้า รวมถึงหน่วยงานที่ต้องติดต่อเพื่อตรวจสอบขอความช่วยเหลือหรือร้องเรียน และประชาสัมพันธ์ให้ประชาชนทราบโดยเร่งด่วนเพื่อสร้างองค์ความรู้ให้กับประชาชนในการรับมือกับกลโกงของมิจฉาชีพ โดยฐานข้อมูลดังกล่าวประกอบด้วย

๑) 5 DO 5 DON’T เพื่อให้ประชาชนทราบสิ่งที่ควรทำและไม่ควรทำหากได้รับการติดต่อจากมิจฉาชีพ

๒) กลลวงมิจฉาชีพที่พบบ่อยเพื่อให้ประชาชนรู้เท่าทัน เช่น กรณีการอ้างเป็นสถาบันการเงิน หรืออ้างเป็นหน่วยงานรัฐ

๓) ช่องทางการแจ้งเบาะแส ได้รวบรวมช่องทางการแจ้งเบาะแสหรือร้องเรียนให้ประชาชนได้รับทราบ

๔) การแก้ไขปัญหาเฉพาะหน้าเมื่อได้รับสายแก๊ง Call Center หรือข้อความสั้นหลอกลวง

๕) เตือนภัย : โทรหลอกลวง และข้อความสั้นหลอกลวง

นอกจากนั้น สำนักงาน กสทช. มีช่องทางการรับแจ้งข้อมูลการหลอกลวงต่าง ๆ ร่วมกับผู้ให้บริการโทรศัพท์เคลื่อนที่ทุกราย และได้ประสานความร่วมมือกับศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์ (ศูนย์ ๑๒๑๒ ETDA) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อเชื่อมต่อข้อมูลเรื่องร้องเรียนการฉ้อโกงผ่านระบบโทรศัพท์เคลื่อนที่และสื่ออิเล็กทรอนิกส์

๑.๕ การบูรณาการงานร่วมกันระหว่างหน่วยงาน

๑) การประสานงานแจ้งข้อมูล SMS หลอกลวง กรณีได้รับเรื่องร้องเรียนหรือการแจ้งเบาะแสจากประชาชนผ่านช่องทางต่าง ๆ โดยการบล็อก SMS ที่มีลักษณะ ชวนให้เล่นการพนัน หลอกลวงสินเชื่อเงินกู้ หลอกโอนเงินเข้าบัญชี ซึ่งสำนักงาน กสทช. จะขอข้อมูลที่จำเป็นให้การตรวจสอบหาผู้กระทำความผิดจากประชาชน ก่อนรวบรวมส่งให้กับผู้รับใบอนุญาต และผู้รับใบอนุญาตจะตรวจสอบและจัดส่งข้อมูลของมิจฉาชีพให้กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีดำเนินการทางกฎหมายต่อไป

๒) การประสานงานแจ้งข้อมูลแก๊ง Call Center หลอกลวง กรณีได้รับเรื่องร้องเรียนหรือแจ้งเบาะแสจากประชาชนผ่านช่องทางต่าง ๆ ซึ่งสำนักงาน กสทช. จะขอข้อมูลที่จำเป็นให้การตรวจสอบหาผู้กระทำความผิดจากประชาชน ก่อนรวบรวมส่งให้กับผู้รับใบอนุญาต และผู้รับใบอนุญาตจะตรวจสอบและจัดส่งข้อมูลของมิจฉาชีพให้กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีดำเนินการทางกฎหมายต่อไป

๒. ธนาคารแห่งประเทศไทย (ธปท.)

ธนาคารแห่งประเทศไทย (ธปท.) เป็นอีกหน่วยงานหนึ่งที่มีบทบาทอย่างมากเรื่องการแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ทั้งในฐานะที่เป็นผู้กำกับดูแลสถาบันทางการเงินซึ่งมีส่วนสำคัญในกระบวนการหลอกลวงของมิจฉาชีพ และในฐานะที่มักเป็นผู้ถูกมิจฉาชีพแอบอ้าง ซึ่ง ธปท. ได้มีความพยายามในการแก้ไขปัญหาอาชญากรรมทางการเงินมาโดยตลอด เช่น ในช่วงปี ๒๕๖๔ ภัยทางเงินจะมาในรูปแบบการหลอกลวงผ่านบัตรเครดิต (BIN Attack) ซึ่งคนร้ายจะใช้รหัส BIN (Bank Identification Number) โดยสุ่มเลขบัตรเครดิตและบัตรเดบิตของลูกค้าและนำไปใช้ทำรายการในร้านค้าในต่างประเทศ ทำให้มีการหักเงินออกจากตัวบัตรเครดิต ซึ่ง ธปท. ก็ได้มีระบบการตรวจจับ Bin Attack เพื่อรับมือกับปัญหาการใช้บัตรเครดิตปลอม ซึ่งทำให้ ปัญหาการหลอกลวงผ่านบัตรเครดิตมีจำนวนลดน้อยลงไปกว่าร้อยละ ๘๘ มูลค่าความเสียหายลดลงไปกว่าร้อยละ ๔๗ ต่อมา การหลอกลวงเปลี่ยนรูปแบบเป็นการหลอกลวงผ่าน SMS และการโทรหรือแก๊งคอลเซ็นเตอร์ แก๊งคอลเซ็นเตอร์ก็จะติดต่อลูกค้าให้ทำรายการโอนเงิน ซึ่งการโอนเงินก็จะไปอยู่ที่ช่องทาง Mobile Banking โดยความเสียหายที่เกิดขึ้นในช่องทาง Mobile banking ของปี ๒๕๖๕ อยู่ที่ประมาณ ๖,๐๐๐ กว่ารายการ หรือเพิ่มขึ้นประมาณร้อยละ ๘๐ จากปี ๒๕๖๔ และมีมูลค่าความเสียหายอยู่ที่ ๒๗๔ ล้านบาท หรือเพิ่มขึ้นถึงร้อยละ ๗๐ จากปี ๒๕๖๔ นอกจากการหลอกลวงในลักษณะที่มีคนร้ายติดต่อไปหลอกลวงผู้เสียหายแล้ว ยังมีกรณีที่คนร้ายใช้แอพพลิเคชั่นดูดเงิน ซึ่งมีความเสียหายนับตั้งแต่กลางปี ๒๕๖๕ ถึงต้นปี ๒๕๖๖ พบว่ามีมูลค่าความเสียหายกว่า ๕๐๐ ล้านบาท ด้วยความเสียหายที่เพิ่มสูงขึ้นมาก ธปท. ได้มีมาตรการเพื่อรับมือกับปัญหาอาชญากรรมออนไลน์ “มาตรการจัดการภัยทุจริตทางการเงิน” รวมทั้งปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ วันที่ ๙ มีนาคม ๒๕๖๖ โดยสามารถแบ่งออกได้เป็น ๓ มาตรการหลักเพื่อจัดการกับข้อบกพร่องของ

การแก้ปัญหาแบบเดิมซึ่งต้องมีการแก้ไขเพิ่มเติม โดย ธปท. มีหลักการที่สำคัญคือให้เป็นมาตรการจัดการภัยทุจริตทางการเงินครอบคลุมด้านการ*ป้องกัน ตรวจจับ ตอบสนองและรับมือ* ซึ่งกำหนดแนวปฏิบัติขั้นต่ำให้ทุกสถาบันการเงินปฏิบัติตามเป็นมาตรฐานเดียวกัน บนหลักการรักษาสมดุลระหว่างการบริหารความเสี่ยง และส่งเสริมบริการทางการเงินดิจิทัล โดยมาตรการทั้ง ๓ ข้อมีดังนี้

๑) ป้องกันความเสี่ยง และปิดช่องโหว่ภัยทางการเงินรูปแบบใหม่ ๆ ได้อย่างเท่าทัน เพื่อแก้ไขจุดบกพร่องในเรื่องที่มิจฉาชีพสามารถเข้าถึงประชาชนผ่านหลายช่องทาง หลายรูปแบบ

๑.๑) ให้ธนาคารงดส่งลิงก์ทุกประเภทผ่าน SMS อีเมล และงดส่งลิงก์ขอข้อมูลสำคัญ เช่น ชื่อผู้ใช้งาน รหัสผ่าน และเลขบัตรประชาชน ผ่านโซเชียลมีเดีย เนื่องจากการดำเนินการที่ผ่านมาจะเป็นการแจ้งให้ประชาชนทราบว่าห้ามกดลิงก์ที่มาใน SMS แต่บางธนาคารก็ยังมีการส่งลิงก์ให้ผู้ใช้บริการผ่าน SMS หรืออีเมล จึงให้ธนาคารลดส่งลิงก์ทุกประเภทให้ผู้ใช้บริการ ทั้งนี้ ในการสื่อสารผ่านสื่อโซเชียลมีเดีย ยังให้มีการส่งลิงก์ได้ แต่ห้ามการขอชื่อผู้ใช้งาน หรือข้อมูลที่เป็นความลับ โดยปัจจุบันธนาคารได้งดการส่งลิงก์ผ่าน SMS ทั้งหมดแล้ว ในส่วนของอีเมลจะดำเนินการให้แล้วเสร็จภายในเดือนมิถุนายน ๒๕๖๖

๑.๒) ปิดกั้น SMS และเบอร์ Call center ที่แอบอ้างเป็นธนาคาร และปิด website หลอกลวง โดยเป็นความร่วมมือกับ กสทช. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสมาคมธนาคารไทย (TB-CERT) โดยตามกระบวนการปกติแล้วนั้น การปิดเว็บไซต์จะต้องมีหมายศาลไปให้กับผู้ให้บริการอินเทอร์เน็ต ซึ่งใช้เวลานาน จึงมีความร่วมมือกันระหว่าง ธปท. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สมาคมธนาคารไทยและยังมีผู้ให้บริการอินเทอร์เน็ต ในการปิดกั้นเว็บไซต์หลอกลวง รวมทั้งการปิดกั้น SMS และเบอร์ Call center ซึ่งเป็นความร่วมมือกับ กสทช. ด้วย

๑.๓) จำกัด ๑ บัญชีผู้ใช้งาน mobile banking (username) ของแต่ละธนาคาร ให้ใช้ได้ใน ๑ อุปกรณ์เท่านั้น เพื่อป้องกันการที่มิจฉาชีพเข้ามาควบคุมระบบโทรศัพท์ทางไกลหรือใช้แอพดูดเงิน ซึ่งอาจจะได้เงินไปจากหลายบัญชี จึงให้โทรศัพท์ ๑ เครื่องสามารถใช้ได้แค่ ๑ บัญชีเพื่อลดความเสี่ยง ในขณะเดียวกันก็ยังสามารถลดจำนวนการใช้งานของบัญชีม้าหลายบัญชีบนโทรศัพท์เครื่องเดียวอีกด้วย

๑.๔) ธนาคารต้องแจ้งเตือนบน mobile banking ก่อนทำธุรกรรมทุกครั้ง และต้องให้ผู้ใช้งานประเมินการตระหนักรู้ต่อภัยทุจริต (awareness test) เป็นระยะ ๆ ในกรณีที่ผู้ใช้บริการถูกหลอกและกำลังจะโอนเงินให้มิจฉาชีพแล้ว ก็จะต้องมีการแจ้งเตือนซึ่งถือว่าเป็นด่านสุดท้ายที่จะช่วยป้องกันผู้ใช้บริการจากความเสียหายได้ โดยต้องให้มีการแจ้งเตือนที่เห็นได้ชัด นอกจากนี้ยังต้องมีการประเมินความรู้โดยเป็นแบบทดสอบใน Mobile banking ให้ผู้ใช้บริการทำอาจกำหนดระยะเวลาทุก ๖ เดือน โดยเป็นการให้ตอบคำถาม ๓ ข้อ ผู้ใช้บริการต้องตอบให้ครบและถูกทั้ง ๓ ข้อ ซึ่งหากตอบผิดหรือไม่ครบ อาจมีผลอาจจะมีผลต่อการกำหนดวงเงินให้เหมาะสมกับระดับความตระหนักรู้ของผู้ใช้บริการ มาตรการทั้ง ๒ ส่วน คาดว่าจะแล้วเสร็จในเดือนมิถุนายน ๒๕๖๖

๑.๕) ธนาคารต้องปรับปรุงระบบรักษาความปลอดภัยบน Mobile banking ให้ทันสมัย เท่าทันภัยการเงินรูปแบบใหม่อยู่เสมอ และให้แล้วเสร็จตามที่ ธปท. กำหนด โดยเฉพาะการตรวจจับว่าในโทรศัพท์ของผู้ใช้บริการได้มีการติดตั้งแอพดูดเงิน หรือพวกมัลแวร์

๑.๖) ธนาคารต้องให้ยืนยันตัวตนขั้นต่ำด้วย biometrics เมื่อเปิดบัญชีแบบ non-face-to-face หรือเมื่อเปลี่ยนวงเงิน หรือเมื่อโอนเงินจำนวนมาก ธปท. พิจารณาว่าการยืนยันตัวตนด้วย Biometrics จะช่วยป้องกันมิจฉาชีพที่ใช้วิธีการควบคุมโทรศัพท์ทางไกลได้ โดยหากผู้ใช้บริการต้องการทำรายการ จะต้องมีการยืนยันตัวตนด้วยการสแกนใบหน้า และเทียบใบหน้านั้นกับใบหน้าที่ทางธนาคารได้บันทึกไว้ อย่างก็ดี การให้ผู้ใช้บริการสแกนใบหน้าทุกครั้งจะสร้างความไม่สะดวกให้กับผู้ใช้บริการ จึงได้มีการกำหนดให้ใช้การสแกนใบหน้ากับรายการที่เป็นการโอนเงินจำนวนมากก่อน

๑.๗) กำหนดเพดานวงเงินถอน/ โอนสูงสุดต่อวันให้เหมาะสมตามระดับความเสี่ยงของกลุ่มผู้ใช้บริการแต่ละประเภท (ลูกค้าสามารถขอปรับได้ตามความจำเป็น และต้องยืนยันตัวตนอย่างเข้มงวด) จากมาตรการข้างต้นที่ให้มีการกำหนดรายการที่เป็นการโอนเงินจำนวนมาก จึงมีการศึกษาว่าเงินเท่าไหร่จึงจะพิจารณาว่าเป็นการโอนเงินจำนวนมาก และได้จำนวนที่ ๕๐,๐๐๐ บาท ต่อรายการ และใน ๑ วันจะทำรายการไม่เกิน ๒๐๐,๐๐๐ บาท หากเกิน ๒๐๐,๐๐๐ บาทจะต้องทำการสแกนใบหน้า และการเปลี่ยนวงเงินทุกครั้งจะต้องมีการสแกนใบหน้าด้วย นอกจากนี้ ยังมีการกำหนดให้หรือผู้ใช้บริการที่อายุต่ำกว่า ๑๕ ปี เป็นผู้ใช้บริการกลุ่มเปราะบาง ทางธนาคารอาจมิให้มีการใช้ Mobile banking หรือกำหนดวงเงิน

๒) ตรวจจับ/ติดตามบัญชี และธุรกรรมต้องสงสัย เพื่อแก้ไขจุดบกพร่องในเรื่องหากพบบัญชีผิดปกติแล้วสถาบันการเงินไม่สามารถอายัดได้ทันที และยังมีการซื้อ-ขายบัญชีม้าอยู่มาก

๒.๑) กำหนดเงื่อนไขการตรวจจับ/ ติดตามธุรกรรมเข้าข่ายผิดปกติ หรือกระทำความผิด และรายงานไป ปปง.

๒.๒) ธนาคารต้องมีระบบตรวจจับ/ ติดตามธุรกรรมเข้าข่ายผิดปกติ แบบ near real-time เพื่อระงับธุรกรรมได้ทันทีที่ตรวจพบ เนื่องจากแต่เดิมการตรวจสอบความผิดปกติจะพบได้แบบวันต่อวัน คือตรวจสอบได้ตอนสิ้นวันซึ่งอาจจะล่าช้าเกินไป จึงมีการกำหนดให้มีการตรวจจับพฤติกรรมแบบ Realtime เพื่อระงับธุรกรรมได้ทันที ธปท. ได้กำหนดให้สามารถใช้งานได้ภายในสิ้นปี ๒๕๖๖

๒.๓) จัดให้มีช่องทางแจ้งความออนไลน์ ร่วมกับสำนักงานตำรวจแห่งชาติ สมาคมธนาคารไทย และสมาคมสถาบันการเงินของรัฐ ทางสำนักงานตำรวจแห่งชาติร่วมกับสมาคมธนาคารไทยก็ได้จัดตั้งหน่วยรับแจ้งความออนไลน์หรือ thaipoliceonline.com ทำให้ลูกค้าสามารถที่จะโทรแจ้งความได้

๓) ตอบสนองและรับมือ ได้ทันท่วงทีเมื่อเกิดเหตุ เพื่อแก้ไขจุดบกพร่องในการแก้ไขปัญหาให้ผู้เสียหายที่ยังล่าช้าทั้งการแจ้งความและการแจ้งสถาบันการเงินเพื่ออายัดบัญชี

๓.๑) ธนาคารต้องมีช่องทางติดต่อเร่งด่วน (hotline) ตลอด ๒๔ ชั่วโมง ธปท. พิจารณาแล้วว่าการติดต่อของผู้เสียหายไปยัง Call center ของแต่ละธนาคารหรือโทรไปหาตำรวจมีความล่าช้า ซึ่งกว่าจะถึงขั้นตอนการระงับธุรกรรมได้ก็ใช้เวลานานเกินไป มิจฉาชีพก็ดำเนินการโยกย้ายเงินออกไปได้หมดแล้ว

๓.๒) ธนาคารต้องสนับสนุนการสอบสวนของเจ้าหน้าที่ตำรวจ เพื่อติดตามสาเหตุและผู้กระทำผิด และกำหนดผู้รับผิดชอบในการดูแลและประสานงานกับหน่วยงานต่าง ๆ โดย

ต้องมีเจ้าหน้าที่รับผิดชอบเฉพาะในการประสานงาน มีความรู้ความเข้าใจ และต้องทำหน้าที่ทั้งการประสานงานกับลูกค้าและเจ้าหน้าที่ตำรวจ

๓.๓) ธนาคารต้องดูแลรับผิดชอบผู้ให้บริการ หากพบว่าความเสียหายเกิดจากข้อบกพร่องของธนาคาร

๓.๔) ธปท. มีศูนย์คุ้มครองผู้ใช้บริการทางการเงิน Call center ๑๒๑๓ เป็นช่องทางรับเรื่องร้องเรียนจากประชาชน

นอกจากมาตรการต่าง ๆ ข้างต้นแล้ว ทาง ธปท. ก็ยังมีศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.) ซึ่งก่อตั้งขึ้นตั้งแต่ปี ๒๕๕๕ โดยเป็นศูนย์รับเรื่องร้องเรียนจากประชาชนที่ได้รับความเสียหายจากภัยทุจริตทางการเงิน และยังเป็นศูนย์ที่ให้ข้อมูลและความรู้แก่ประชาชนอีกด้วย อย่างไรก็ดี การดำเนินการของ ธปท. เพียงอย่างเดียวไม่เพียงพอที่จะแก้ไขจุดบกพร่องในการแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ได้ทั้งหมด จำเป็นต้องใช้กลไกอื่นประกอบด้วย โดยข้อบกพร่องที่ยังเหลืออยู่ เช่น การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องเพื่อใช้ในการสืบสวนสอบสวน การอายัดบัญชีที่ยังมีความล่าช้าและยุ่งยาก และบทลงโทษการเปิดหรือซื้อ-ขายบัญชีม้าและซิมม้าที่ยังไม่ชัดเจน โดยข้อจำกัดเหล่านี้ได้มีการแก้ไขปรับปรุงด้วยการใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ดังที่ได้มีการอธิบายในเรื่องกฎหมายที่เกี่ยวข้อง

ปัญหาและอุปสรรคในการดำเนินการ

แม้ว่าหน่วยงานที่เกี่ยวข้องจะมีการกำหนดมาตรการต่าง ๆ เพื่อรับมือกับปัญหาหลายข้อ อย่างไรก็ดี ในการดำเนินการตามมาตรการก็ยังคงมีปัญหาและอุปสรรค ซึ่งส่งผลกระทบให้การแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สำเร็จได้ยากขึ้น โดยปัญหาและอุปสรรคในการดำเนินการของหน่วยงานที่เกี่ยวข้องสามารถสรุปได้ดังนี้

๑. กระบวนการในการแก้ไขปัญหา

เนื่องจากก่อนมีการประกาศใช้ พ.ร.ก. อาชญากรรมทางเทคโนโลยี ในกระบวนการแก้ไขปัญหายังมีข้อจำกัดในเรื่องการบังคับใช้กฎหมาย ทำให้กระบวนการสืบสวนสอบสวนจนถึงการจับกุมผู้กระทำผิดทำได้ยากและใช้เวลามาก เช่น การระงับธุรกรรมทางการเงินที่ต้องสงสัยว่ามีความเกี่ยวข้องกับอาชญากรรม รวมทั้งการระงับบัญชีต้องสงสัยยังไม่สามารถทำได้โดยง่าย การซื้อขายบัญชีม้า การแจ้งความร้องทุกข์ที่ยังติดขัดในเรื่องการระบุสถานที่เกิดเหตุ ซึ่งด้วยข้อจำกัดเหล่านี้ทำให้การแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ได้ยาก อย่างไรก็ดี ปัญหาดังกล่าวได้มีการใช้ พ.ร.ก. ดังกล่าวเข้ามาช่วยแก้ปัญหาได้มากขึ้น

๒. การพัฒนาวิธีการหลอกลวงอย่างรวดเร็วของมิจฉาชีพ

มิจฉาชีพในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่นับได้ว่าเป็นกลุ่มผู้กระทำผิดที่มีการปรับตัวอย่างรวดเร็ว โดยมีการพัฒนาวิธีการต่าง ๆ และปรับเปลี่ยนได้ทันท่วงที เช่น การที่หน่วยงานของรัฐเริ่มใช้มาตรการระงับสายเรียกเข้าจากต่างประเทศ มิจฉาชีพก็หันไปใช้การโทรผ่าน Simbox แทน หรือการใช้การส่งข้อความผ่าน SMS เริ่มมีการปิดกั้น ก็หันไปใช้การส่งข้อความผ่านสื่อ

โซเชียลมีเดียมากขึ้น ในขณะที่มิจฉาชีพสามารถปรับเปลี่ยนรูปแบบการหลอกลวงได้อย่างรวดเร็ว หน่วยงานที่เกี่ยวข้องหรือหน่วยงานรัฐไม่สามารถปรับเปลี่ยนวิธีการรับมือได้ทัน เนื่องด้วยความติดขัดทางด้านระเบียบวิธี กฎหมายต่าง ๆ ทำให้การมีมาตรการใหม่มักออกมาในเวลาที่ความเสียหายได้เกิดขึ้นเป็นวงกว้างแล้ว อีกทั้งนอกจากการโทรหาเป้าหมายแล้ว มิจฉาชีพยังมีการใช้แอพดูดเงินหรือเทคโนโลยีต่าง ๆ เข้ามาช่วย ซึ่งเป็นอีกข้อจำกัดหนึ่งของหน่วยงานที่รับผิดชอบที่ต้องพัฒนาเทคโนโลยีในการตรวจจับให้ทัน ซึ่งต้องใช้ทั้งเวลาและบุคลากรที่มีความรู้ด้วย

๓. มิจฉาชีพตั้งฐานปฏิบัติการในต่างประเทศ

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มีปัญหาและอุปสรรคใหญ่และมักมีการกล่าวถึงเสมอคือการที่ฐานปฏิบัติการของกลุ่มมิจฉาชีพอยู่ในต่างประเทศ โดยเฉพาะในเขตชายแดนประเทศเพื่อนบ้านของไทย ซึ่งการที่ผู้กระทำผิดอยู่ในต่างประเทศทำให้ไม่สามารถจับกุมคนร้ายได้ในทันที ด้วยข้อจำกัดของกฎหมายไทยที่ไม่สามารถบังคับใช้ในต่างประเทศและการเข้าไปยังต่างประเทศยังอาจเป็นการรุกล้ำอำนาจอธิปไตยของประเทศอื่นด้วย ดังนั้น ในการจับกุมจึงต้องได้รับความยินยอมจากประเทศนั้นและยังต้องอาศัยความร่วมมือจากเจ้าหน้าที่ในประเทศนั้นเป็นอย่างมาก ด้วยเหตุนี้ การจับกุมจึงทำได้ยากและมีจำนวนน้อยเมื่อเทียบกับจำนวนกรณีที่มีการร้องเรียนและความเสียหายที่เกิดขึ้น

๔. การถ่วงดุลระหว่างผลประโยชน์ของประชาชนและการป้องกันปัญหา

อาจกล่าวได้ว่าปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นปัญหาที่อาศัยช่องว่างของเทคโนโลยี ช่องว่างของความพยายามในการอำนวยความสะดวกให้แก่ประชาชนและหน่วยธุรกิจในประเทศไทย เช่น การมีสัญญาณอินเทอร์เน็ตที่เร็วและแรงจนถึงเขตประเทศเพื่อนบ้าน การใช้ Mobile banking ซึ่งทำให้ประชาชนผู้ใช้บริการได้รับความสะดวกสบายในการทำธุรกรรมทางการเงินผ่านโทรศัพท์เคลื่อนที่ของตนในเวลาอันรวดเร็ว และยังทำให้เกิดสังคมไร้เงินสด (Cashless society) ได้ แต่ความสะดวกสบายนั้นมิได้มีให้เฉพาะกลุ่มผู้ใช้บริการเท่านั้น ทั้งยังเป็นการอำนวยความสะดวกให้แก่มิจฉาชีพได้อีกด้วย มิจฉาชีพสามารถโยกย้ายเงินออกจากบัญชีม้าได้อย่างรวดเร็วและไม่จำเป็นต้องเสี่ยงเดินทางไปยังตู้ ATM หรือไปที่สาขาของธนาคาร นอกจากนี้ การที่มีระบบ Mobile Banking ที่รวดเร็วนั้น ยังทำให้ประชาชนไม่มีเวลาตรึกตรองสถานการณ์เมื่อถูกหลอกได้ และโอนเงินให้กับมิจฉาชีพได้โดยไม่ทันคิด ซึ่งเมื่อกว่าจะรู้ตัว เงินที่โอนก็ถูกโยกย้ายไปหลายบัญชีจนยากที่จะติดตามได้

เมื่อจำเป็นต้องมีมาตรการต่าง ๆ ออกมาเพื่อคุ้มครองประชาชนจากการถูกหลอก ก็พบว่าหลายมาตรการอาจกระทบต่อความสะดวกสบายของประชาชนได้ เช่น การใช้การสแกนใบหน้าเมื่อมีการทำรายการผ่าน Mobile Banking ซึ่งกระทบกับประชาชนทั่วไปที่ต้องการทำรายการ หรือการต้องมีแบบทดสอบให้ผู้ใช้บริการทำ แม้ว่าจะเป็นการสร้างความตระหนักรู้ให้กับผู้ใช้บริกา รแต่ก็พิจารณาได้ว่าเป็นการสร้างความยุ่งยากให้กับประชาชนได้ นอกจากนี้ การดำเนินมาตรการที่เด็ดขาดก็อาจกระทบต่อสิทธิและเสรีภาพของประชาชนได้ เช่น ในกรณีที่มีการร้องเรียนเลขหมายโทรศัพท์ที่เป็นเลขหมายของมิจฉาชีพ การดำเนินการระงับเลขหมายนั้นโดยทันที อาจทำให้เจ้าของเลขหมายที่อาจไม่ได้เป็นมิจฉาชีพต้องเสียสิทธิ์ในการใช้เลขหมายนั้น เป็นต้น

ดังนั้น อุปสรรคของการแก้ปัญหาการหลอกลวงผ่านโทรศัพท์เคลื่อนที่ประการหนึ่งคือการที่หน่วยงานที่เกี่ยวข้องต้องถ่วงดุลระหว่างผลประโยชน์ ความสะดวกสบาย สิทธิเสรีภาพของประชาชน กับการปกป้องประชาชนจากมิจฉาชีพที่อาจทำให้เกิดการรุกล้ำความเป็นส่วนตัวของประชาชน ทำให้เกิดความไม่สะดวกสบาย หรืออาจเป็นการสร้างภาระให้ผู้ใช้บริการ

๕. การขาดความร่วมมือของหน่วยงานต่าง ๆ อย่างครบถ้วน

ก่อนมีการบังคับใช้ พ.ร.ก. อาชญากรรมทางเทคโนโลยีนั้น มีปัญหาและอุปสรรคในเรื่องของบทบาทและหน้าที่ของหน่วยงานที่เกี่ยวข้อง โดยการที่หน่วยงานต่าง ๆ ต่างก็ไม่สามารถดำเนินการได้มากด้วยติดขัดในเรื่องกฎหมายและกฎระเบียบ การไม่สามารถเปิดเผยข้อมูลได้เท่าที่ควร ทำให้การดำเนินการล่าช้า โดย พ.ร.ก. ได้มีการกำหนดหน้าที่ของหน่วยงานต่าง ๆ โดยเฉพาะเรื่องการแบ่งปันข้อมูลอย่างชัดเจน ทำให้ความร่วมมือระหว่างหน่วยงานได้อย่างถูกต้องมากขึ้น อย่างไรก็ดี ยังพบว่ามีปัญหาและอุปสรรคในความร่วมมือระหว่างหน่วยงาน โดยยังมิได้มีการกำหนดว่าหน่วยงานใดควรเป็นหน่วยงานกลางในการดำเนินการของหน่วยงานต่าง ๆ กล่าวคือ ยังไม่มีเจ้าภาพ ซึ่งอาจแก้ไขได้ด้วยการตกลงกันระหว่างหน่วยงานได้ ทั้งนี้ ใน พ.ร.ก. ได้กำหนดตำแหน่งหน้าที่ของคณะกรรมการโดยกำหนดให้รัฐมนตรีกระทรวงดิจิทัลเพื่อเศรษฐกิจสังคม

๖. ข้อจำกัดของการกำกับดูแลบริการโอทีที

ปัจจุบัน บริการโอทีทีหรือบริการแอพพลิเคชั่นต่าง ๆ ยังไม่มีการกำกับดูแลโดยสำนักงาน กสทช. ซึ่งการที่ยังไม่มีการกำกับดูแลยังหมายถึงการที่หน่วยงานในไทยยังไม่มีอำนาจที่จะควบคุมการดำเนินงาน การเข้าถึงข้อมูลต่าง ๆ ที่อยู่บนแอพพลิเคชั่นเหล่านี้ได้อีกด้วย เมื่อไม่สามารถเข้าถึงข้อมูลและไม่สามารถควบคุมได้ ทำให้เจ้าหน้าที่ที่เกี่ยวข้องไม่สามารถจัดการกับการหลอกลวงที่เกิดขึ้นบนการสื่อสารผ่านแอพพลิเคชั่นดังกล่าวได้ ซึ่งต้องอาศัยการดำเนินการของบริษัทเจ้าของแอพพลิเคชั่นนั้นเป็นหลัก จึงไม่สามารถคาดการณ์ผลลัพธ์ที่จะเกิดขึ้นได้

เมื่อได้มีการศึกษาและประมวลปัญหาและอุปสรรคจากการดำเนินการที่ผ่านมาของหน่วยงานที่เกี่ยวข้อง ซึ่งมีผลกระทบต่อการแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่นั้น ก็จะสามารถพิจารณาถึงแนวทางในการแก้ไขปรับปรุงมาตรการเพื่อรับมือกับปัญหาได้ดียิ่งขึ้น ซึ่งจะเป็นการวิเคราะห์ที่สำคัญในส่วนต่อไป

สรุป

จากการรวบรวมข้อมูลทั้งข้อมูลปฐมภูมิและทุติยภูมิ ด้วยการการสัมภาษณ์หน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน และด้วยการค้นคว้าจากเอกสารที่เกี่ยวข้องต่าง ๆ จะเห็นได้ว่าการหลอกลวงผ่านโทรศัพท์เคลื่อนที่ในประเทศไทยมีความรุนแรงของปัญหาค่อนข้างมาก โดยประเมินจากจำนวนกรณีที่มีการร้องเรียนและมูลค่าความเสียหายโดยรวม จึงเป็นเหตุผลสำคัญของการศึกษาในรายละเอียดของลักษณะการหลอกลวงรวมทั้งองค์ประกอบของการหลอกลวง และมาตรการต่าง ๆ ที่มีอยู่ในปัจจุบัน เพื่อนำเสนอมาตรการรับมือและแก้ไขที่เหมาะสมในบทถัดไป จากการศึกษา พบว่ามิจฉาชีพในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มีการทำงานเป็นขบวนการที่ตั้งฐานปฏิบัติการในประเทศเพื่อนบ้านของไทย ขบวนการดังกล่าวประกอบด้วยมิจฉาชีพที่ทำหน้าที่ติดต่อหา

เป้าหมายเพื่อหลอกลวงด้วยหลักการทางจิตวิทยาต่าง ๆ มิจฉาชีพกลุ่มที่ทำหน้าที่สนับสนุนและดูแลระบบ จัดหาอุปกรณ์และเครื่องมือต่าง ๆ รวมทั้งซิมม้าและบัญชีม้าด้วย และกลุ่มนายทุนที่ทำหน้าที่รับผิดชอบต้นทุนที่เกิดขึ้นและผลักดันให้ขบวนการหลอกลวงขับเคลื่อนต่อไปได้ ในส่วนของขั้นตอนการหลอกลวงนั้น มิจฉาชีพได้ดำเนินการอย่างเป็นระบบตั้งแต่การเตรียมการต่าง ๆ การหลอกลวงเป้าหมาย ไปจนถึงการจัดการการโยกย้ายเงินไปยังมิจฉาชีพโดยมิให้เจ้าหน้าที่ตำรวจติดตามจับกุมได้โดยง่าย โดยการทำงานของมิจฉาชีพนี้ อยู่ภายใต้ปัจจัยแวดล้อมที่เอื้ออำนวยกับการหลอกลวง ทั้งการที่อำนาจของกฎหมายไทยไม่สามารถเข้าถึงฐานปฏิบัติการของมิจฉาชีพที่ตั้งอยู่ในต่างประเทศได้ ซึ่งทำให้การติดตามจับกุมจึงทำได้ยาก การที่เทคโนโลยีสมัยใหม่อำนวยให้มิจฉาชีพสามารถเข้าถึงเป้าหมายได้อย่างรวดเร็วและมีต้นทุนต่ำ การที่หน่วยงานและบริษัทต่าง ๆ อำนวยความสะดวกให้ผู้ใช้บริการอย่างการให้มีการทำธุรกรรมทางการเงินผ่าน Mobile Banking ซึ่งความสะดวกสบายเหล่านี้ไม่ได้เกิดขึ้นเฉพาะกับผู้ใช้บริการ หากแต่ยังเป็นการอำนวยความสะดวกสบายให้มิจฉาชีพอีกด้วย ด้วยปัจจัยแวดล้อมเหล่านี้ ทำให้ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ขยายตัวเป็นวงกว้างแต่สามารถจัดการได้น้อยกว่าที่ควร

แม้ว่าปัญหาดังกล่าวจะสามารถแก้ไขได้ยาก แต่หน่วยงานที่เกี่ยวข้องก็มีมาตรการหรือแนวทางในการรับมือที่แข็งขัน เช่น สำนักงาน กสทช. ที่จัดให้มีการปิดกั้นการเข้าถึงของมิจฉาชีพทางโทรศัพท์ด้วยวิธีการต่าง ๆ ธปท. ที่ให้มีการทำธุรกรรมทางการเงินผ่าน Mobile Banking ที่รัดกุมมากขึ้น บช.สอท. ที่ผลักดันให้มีการบังคับใช้กฎหมายต่อต้านอาชญากรรมทางเทคโนโลยี และหน่วยงานภาคเอกชนที่จัดให้มีระบบการร้องเรียนต่าง ๆ สำหรับผู้ใช้บริการ อย่างไรก็ดี แม้ว่าจะมีการกำหนดมาตรการหรือแนวทางในการแก้ปัญหาจากหลายหน่วยงาน แต่ก็ยังมีอุปสรรคและข้อจำกัดต่าง ๆ อยู่ เช่น ข้อจำกัดทางเทคนิค การปรับตัวอย่างรวดเร็วของมิจฉาชีพ ข้อจำกัดในเรื่องการตั้งฐานปฏิบัติการในต่างประเทศของมิจฉาชีพ เป็นต้น โดยจะได้มีการวิเคราะห์ถึงมาตรการที่มีในปัจจุบัน อุปสรรคต่าง ๆ และพิจารณาแนวทางที่เหมาะสมเพื่อใช้เป็นข้อเสนอในการรับมือและแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยในบทต่อไป

บทที่ ๔
แนวนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศนับเป็นปัญหาใหญ่ และได้มีความพยายามในการแก้ปัญหาทั้งจากภาครัฐและเอกชน โดยมีการออกมาตรการต่าง ๆ หลายประการ แม้ว่าปัจจุบันนับได้ว่า มีการแก้ปัญหามากมาย แต่ก็อาจยังไม่เพียงพอต่อการทำให้ปัญหาหมดไปได้ และอาจยังไม่รอบด้านครบทุกองค์ประกอบของการแก้ปัญหาที่สำคัญ ในบทนี้จึงเป็นการวิเคราะห์และประเมินว่าแนวทางหรือมาตรการที่มีการใช้อยู่ในปัจจุบันเพียงพอและจะสามารถนำไปสู่เป้าหมายของการแก้ปัญหาหรือไม่ อย่างไร โดยข้อมูลที่ใช้ในการวิเคราะห์มาจากการรวบรวมจากแหล่งข้อมูลปฐมภูมิ คือการสัมภาษณ์หน่วยงานที่เกี่ยวข้อง ดังที่ได้มีการนำเสนอในบทที่ ๓ และแหล่งข้อมูลทุติยภูมิ ซึ่งได้รับจากการรวบรวมจากเอกสาร หนังสือ และกรณีศึกษาต่างประเทศ ดังที่ได้มีการนำเสนอในบทที่ ๒ และบทที่ ๓ ข้อมูลที่ได้รับจะนำมาวิเคราะห์โดยใช้การวิเคราะห์ช่องว่าง (Gap Analysis) เมื่อได้รับผลการศึกษาแล้ว ก็จะสามารถนำเสนอมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ จุดประสงค์สำคัญที่สุดของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่คือการที่สามารถกำจัดปัญหาดังกล่าวหมดไปจากประเทศไทย และป้องกันมิให้มีการหลอกลวงเกิดขึ้นได้สำเร็จ เพื่อให้ประชาชนอยู่ดีมีสุข มีความปลอดภัยในชีวิตและทรัพย์สิน มีความมั่นคง ตามที่ได้มีการกำหนดไว้ในยุทธศาสตร์ชาติ ๒๐ ปี

การวิเคราะห์ในบทนี้จะแบ่งออกเป็น ๒ ขั้นตอน คือ ๑) การวิเคราะห์ช่องว่างของรูปแบบและพฤติกรรมการหลอกลวงกับการดำเนินมาตรการในการแก้ไขและป้องกันปัญหา ซึ่งจะเป็นการวิเคราะห์ว่าในแต่ละขั้นตอนของการกระทำผิดนั้น ได้มีการกำหนดมาตรการอย่างไร ๒) การวิเคราะห์ช่องว่างของมาตรการที่มีอยู่ในปัจจุบันกับมาตรการตามเป้าหมายของการแก้ปัญหาในแต่ละส่วนของการกระทำผิด โดยการวิเคราะห์ช่องว่างของมาตรการในปัจจุบันยังนำไปสู่การเสนอแนะแนวทางในการปรับปรุงมาตรการที่มีอยู่ให้สามารถแก้ไขและป้องกันปัญหาการหลอกลวงได้อย่างมีประสิทธิภาพมากขึ้น

ข้อวิเคราะห์ช่องว่าง (Gap Analysis) เพื่อหาความแตกต่างระหว่างรูปแบบและพฤติกรรมการหลอกลวงกับการดำเนินมาตรการในการแก้ไขและป้องกันปัญหา

เมื่อพิจารณาถึงลักษณะของรูปแบบและพฤติกรรมการหลอกลวงและการปัญหาและมาตรการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ งานศึกษานี้ได้ใช้การจัดกลุ่มองค์ประกอบของการกระทำผิดตามทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ในการอธิบายถึงการกระทำผิด โดยองค์ประกอบดังกล่าวประกอบด้วย ๓ ส่วน ได้แก่ ผู้กระทำผิด ผู้เสียหาย และโอกาสหรือช่องทางในการกระทำผิด ในส่วนนี้จะอธิบายถึงองค์ประกอบการกระทำผิดทั้ง ๓ ส่วน โดยจะมีการสรุปลักษณะสำคัญของรูปแบบและพฤติกรรมการหลอกลวงจากการประมวลทั้ง ๓ ส่วน จากนั้นจะเป็นการวิเคราะห์ถึงรูปแบบพฤติกรรมการหลอกลวงกับมาตรการในปัจจุบัน เพื่อหาช่องว่างของทั้งสองส่วน เพื่อนำไปสู่การวิเคราะห์ในเรื่องมาตรการที่เหมาะสมต่อไป

๑. ผู้กระทำผิด

จากข้อมูลที่ได้นำเสนอในบทที่ ๓ จะเห็นได้ว่าผู้กระทำผิดมีลักษณะเป็นขบวนการหรือการทำงานเป็นทีมโดยแบ่งหน้าที่กันทำอย่างชัดเจน โดยส่วนใหญ่แล้ว สามารถแบ่งออกเป็น ๓ กลุ่มหลัก คือ ๑) กลุ่มผู้กระทำผิดที่ทำหน้าที่ติดต่อเป้าหมายและใช้วิธีการทางจิตวิทยาในการหลอกลวงเป้าหมายให้โอนเงินให้ ๒) กลุ่มสนับสนุนที่ทำหน้าที่จัดหาและจัดเตรียมอุปกรณ์ที่จำเป็นในการติดต่อเป้าหมาย และหาช่องทางในการโยกย้ายทรัพย์สินไปยังกลุ่มมิจฉาชีพ และ ๓) กลุ่มนายทุนที่ทำหน้าที่ลงทุน รับผิดชอบค่าใช้จ่าย และขับเคลื่อนให้การกระทำผิดดำเนินต่อไป จากข้อเท็จจริงรวมทั้งข้อมูลที่ได้รวบรวม ผู้กระทำผิดมีแรงจูงใจที่สำคัญที่สุดคือการได้มาซึ่งทรัพย์สินของผู้อื่น แม้ว่าอาจมีปัจจัยอื่นร่วมด้วย เช่น ความจำเป็นในชีวิต ข้อจำกัดของทางเลือกในการหารายได้ การขาดสภาพคล่องทางการเงิน แต่ปัจจัยเหล่านี้อาจไม่ใช่สาเหตุที่สำคัญที่สุดและยังมีข้อมูลไม่เพียงพอต่อการสนับสนุนสมมติฐานดังกล่าว นอกจากเรื่องของแรงจูงใจแล้ว ยังพบว่ามีเหตุผลสนับสนุนที่ทำให้การกระทำผิดยังคงดำรงอยู่คือการที่ผู้กระทำผิดไม่มีความเกรงกลัวต่อการถูกจับกุม เพราะได้มีการวางแผนมาเป็นอย่างดีโดยใช้ข้อจำกัดหรือช่องว่างทางกฎหมายและเทคโนโลยี ทั้งการเลือกฐานปฏิบัติการที่อยู่ในต่างประเทศ โดยเฉพาะบริเวณประเทศเพื่อนบ้าน ในลักษณะเหมือนการกระทำผิดขององค์กรข้ามชาติ การดำเนินธุรกรรมทางการเงินผ่าน Mobile Banking ซึ่งทำให้มิจฉาชีพทำธุรกรรมได้อย่างรวดเร็วและติดตามได้ยาก เหตุผลเหล่านี้จึงเป็นส่วนสำคัญที่ทำให้มีผู้กระทำผิดในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เพิ่มจำนวนมากขึ้นและไม่มีแนวโน้มที่จะลดลง

๒. ผู้เสียหาย

จากการรวบรวมข้อมูล พบว่าผู้เสียหายในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สามารถเป็นใครก็ได้ ทุกเพศทุกวัย ทุกอาชีพ ไม่มีความสัมพันธ์โดยตรงกับความรู้ความสามารถ และหน้าที่การงาน แม้ว่าจะมีข้อสังเกตว่าเป็นผู้ที่มีความบกพร่องบางประการในชีวิต เช่น การขาดความรัก ขาดการยอมรับ เป็นคนเชื่อคนง่ายกว่าปกติก็ตาม แต่ก็กล่าวได้ว่า ผู้เสียหายมีความหลากหลายและไม่อาจคาดการณ์ล่วงหน้าได้ง่าย เนื่องด้วยเหตุผลที่สำคัญคือการที่มิจฉาชีพใช้

หลักการทางจิตวิทยาในการหลอกลวงเป้าหมาย ซึ่งเป็นการโจมตีจุดอ่อนของเป้าหมายทั้งในเรื่องจิตใจและกระบวนการตัดสินใจที่อาจผิดพลาดได้ตามแต่สถานการณ์

๓. โอกาสและช่องทางในการกระทำผิด

การกระทำผิดสามารถเกิดขึ้นได้สำเร็จเมื่อมีโอกาส โอกาสในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มีลักษณะที่ต่างจากอาชญากรรมโดยทั่วไป เพราะอาชญากรรมโดยทั่วไปนั้นโอกาสมักประกอบด้วยเวลาและสถานที่ แต่โอกาสในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สามารถพิจารณาได้ว่าเป็นช่องทางในการเข้าถึงประชาชนของมิจฉาชีพ หรือการติดต่อหาเป้าหมายได้ จากนั้นจึงเป็นหลอกลวงโดยใช้วิธีการทางจิตวิทยาต่าง ๆ การติดต่อดังกล่าวกระทำผ่านช่องทางการสื่อสารต่าง ๆ โดยเฉพาะทางโทรศัพท์ โดยอาจเป็นการใช้ซิมการ์ดของไทยโทรหาเป้าหมายจากประเทศเพื่อนบ้าน การใช้การโทรแบบ VoIP และการโทรโดยใช้ Sim box ร่วมด้วย ซึ่งวิธีการเหล่านี้เป็นโอกาสที่มิจฉาชีพสามารถติดต่อ พูดคุย และหลอกลวงประชาชนได้ นอกจากโอกาสในการติดต่อหาเป้าหมายแล้ว ยังมีโอกาสในแง่ของการที่ผู้กระทำผิดสามารถได้รับทรัพย์สินของผู้เสียหายโดยใช้การโอนเงินผ่านบัญชีม้า หรือใช้ Mobile Banking ในการทำธุรกรรมทางการเงินอย่างรวดเร็ว ซึ่งโอกาสหรือช่องทางเหล่านี้เป็นสิ่งที่มิจฉาชีพได้วางแผนมาเป็นอย่างดี โดยใช้ช่องทางของการอำนวยความสะดวกให้แก่ผู้บริโภคของสถาบันการเงินต่าง ๆ

เมื่อพิจารณาภาพรวมของการกระทำผิดจากทั้ง ๓ องค์ประกอบข้างต้น พบว่าการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มีลักษณะสำคัญของการกระทำผิด ๖ ข้อซึ่งรวมถึงการดำเนินการของผู้เสียหายด้วย งานศึกษานี้ได้วิเคราะห์ช่องว่าง (Gap Analysis) ระหว่างลักษณะสำคัญทั้ง ๖ ข้อกับมาตรการที่มีการดำเนินการในปัจจุบัน พบว่าหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนได้มีแนวทางหรือมาตรการหลายประการเพื่อแก้ไขและป้องกันปัญหาดังกล่าว โดยมาตรการได้รวมถึงแนวทางที่มีอยู่เดิมแล้วซึ่งขึ้นมิได้เฉพาะเจาะจงในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เท่านั้น และแนวทางที่ได้กำหนดขึ้นเพื่อนำมาแก้ไขปัญหาดังกล่าวโดยเฉพาะลักษณะสำคัญของรูปแบบและพฤติกรรมการหลอกลวงและมาตรการที่มีในปัจจุบัน มีดังนี้

๑) มิจฉาชีพมีการทำงานเป็นกลุ่มขบวนการ โดยแบ่งหน้าที่กันทำอย่างชัดเจน ในปัจจุบันได้มีการพิจารณามาตรการและแนวทางการแก้ไขและป้องกันปัญหาในเรื่องดังกล่าวมากขึ้น เนื่องจากโดยทั่วไปแล้ว การกระทำผิดในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ได้เป็นความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา ซึ่งเป็นกฎหมายที่มีอยู่เดิมและใช้กับการฉ้อโกงที่หลากหลาย อย่างไรก็ดี ในปัจจุบันได้มีการพิจารณาในเรื่องกลุ่มของมิจฉาชีพอื่น ๆ ที่มีส่วนทำให้การกระทำผิดบรรลุผล เช่น กลุ่มสนับสนุนที่จัดหาซื้อขายซิมม้าและบัญชีม้า โดยกลุ่มเหล่านี้มีโทษตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี จึงกล่าวได้ว่าได้มีมาตรการหรือแนวทางในแก้ไขและป้องกันปัญหาดังกล่าวแล้ว จึงไม่มีช่องว่างในส่วนนี้

๒) มิจฉาชีพมีการตั้งฐานปฏิบัติการในต่างประเทศและมีลักษณะเหมือนอาชญากรรมข้ามชาติ โดยเฉพาะพื้นที่ชายแดนประเทศเพื่อนบ้านของไทย เพื่อหลบหนีการจับกุมจากเจ้าหน้าที่ตำรวจไทยเนื่องด้วยกฎหมายของไทยไม่สามารถบังคับใช้ได้นอกราชอาณาจักร รวมทั้งกระบวนการจับกุมยังทำได้ยาก ปัจจุบันพบว่ามีมาตรการหรือแนวทางในการแก้ไขปัญหาแล้วเช่นกัน โดยแนวทางหรือมาตรการที่มีอยู่แล้วคือสนธิสัญญาส่งผู้ร้ายข้ามแดนของไทยและประเทศเพื่อนบ้าน

แม้ในทางปฏิบัติ การดำเนินการค่อนข้างยุ่งยากและใช้เวลานาน นอกจากนี้ ยังมีการประสานความร่วมมือระหว่างเจ้าหน้าที่ตำรวจของไทยและประเทศเพื่อนบ้านเพื่อการดำเนินการจับกุมผู้กระทำผิดเป็นการเฉพาะกิจ ถึงแม้ว่ามาตรการหรือแนวทางดังกล่าวอาจยังไม่ใช่วิธีที่มีประสิทธิภาพมากนัก แต่ก็จัดได้ว่ามีมาตรการแล้ว จึงไม่มีช่องว่างในเรื่องดังกล่าว

๓) มิจฉาชีพสามารถจัดหาช่องทางและอุปกรณ์ต่าง ๆ ที่ใช้ในการสื่อสารเพื่อเข้าถึงเป้าหมายได้หลายวิธี โดยเฉพาะการใช้ซิมการ์ดหรือซิมม้า ปัจจุบันมีมาตรการหรือแนวทางจากสำนักงาน กสทช. เป็นหลัก โดยได้มีการกำหนดนโยบายให้ผู้ใช้บริการสามารถลงทะเบียนซิมด้วยตนเองหรือผ่านลูกตู้ได้ไม่เกิน ๕ ซิม หากต้องการลงทะเบียนมากกว่า ๕ ซิม จะต้องดำเนินการที่ศูนย์ให้บริการของผู้ให้บริการโทรศัพท์นั้น ๆ เท่านั้น ซึ่งจะเป็นการขัดขวางให้มิจฉาชีพให้สามารถครอบครองซิมการ์ดได้น้อยลง นอกจากนี้ ยังมีมาตรการในเชิงรุกต่าง ๆ เพื่อให้มีการตรวจสอบพฤติกรรมการใช้ซิมการ์ดหรืออุปกรณ์ในการหลอกลวงด้วย เช่น การตรวจจับทราฟฟิกการสื่อสารที่ผิดปกติ ดังนั้น ในรูปแบบการกระทำผิดในข้อนี้จึงจัดว่ามีมาตรการแล้วและไม่มีช่องว่างระหว่างการกระทำผิดและมาตรการแก้ไขและป้องกันปัญหาการหลอกลวง

๔) มิจฉาชีพได้ใช้หลักการหลอกลวงทางจิตวิทยาต่าง ๆ เพื่อโจมตีจุดอ่อนของเป้าหมาย ทั้งใช้การแอบอ้างเป็นเจ้าหน้าที่รัฐให้มีความน่าเชื่อถือ การแอบอ้างเป็นเจ้าหน้าที่ตำรวจและข่มขู่ด้วยคดีร้ายแรงเพื่อให้เป้าหมายเกิดความหวาดกลัว การแอบอ้างเป็นเพื่อนเพื่อให้เป้าหมายเกิดความไว้ใจ ในประเด็นนี้นั้น ได้มีมาตรการในหลายรูปแบบ ส่วนแรกคือการให้ความตระหนักรู้แก่ประชาชนผ่านช่องทางสื่อสารต่าง ๆ เช่น ฐานข้อมูลของสำนักงาน กสทช. และ ธปท. การประชาสัมพันธ์ผ่านช่องทางออนไลน์ต่าง ๆ ของสำนักงานตำรวจแห่งชาติ อย่างไรก็ดี การสร้างความตระหนักรู้เพียงอย่างเดียวอาจไม่เพียงพอ เพราะมิจฉาชีพเน้นโจมตีจุดอ่อนทั้งในเรื่องจิตใจและกระบวนการตัดสินใจของเป้าหมาย จึงต้องมีมาตรการในส่วนที่สอง คือ การปกป้องคุ้มครองประชาชนเพื่อมิให้มีการติดต่อกับมิจฉาชีพตั้งแต่ต้น มาตรการดังกล่าวมีทั้งการปิดกั้นโอกาสที่มิจฉาชีพจะเข้าถึงเป้าหมายหรือประชาชนตั้งแต่ต้น เช่น การระงับทราฟฟิการโทรเข้าจากต่างประเทศซึ่งเป็นการโทรที่สงสัยได้ว่ามาจากมิจฉาชีพ การให้มีแอปพลิเคชันช่วยตรวจจับและแจ้งเตือนผู้ใช้บริการว่าสายเรียกเข้าสายนั้น ๆ อาจเป็นมิจฉาชีพได้ การแจ้งเตือนผู้ใช้บริการโทรศัพท์โดยการใส่ Prefix +๖๙๗ เพื่อให้ประชาชนระมัดระวังสายเรียกเข้าจากต่างประเทศ การใช้ Sender name ใน SMS เป็นต้น

นอกจากนี้ ยังพบว่ามีมาตรการอีกจำนวนหนึ่งของหน่วยงานที่มีความเกี่ยวข้องกับการหลอกลวง เช่น ธปท. ที่พบว่าสถาบันการเงินหรือธนาคารต่าง ๆ มักถูกแอบอ้างจากมิจฉาชีพบ่อยครั้ง จึงมีมาตรการให้มีการปิดกั้นเลขหมายของมิจฉาชีพที่แอบอ้างเป็นเจ้าหน้าที่ธนาคาร และยังมีการจัดทำช่องทางในการร้องเรียนของผู้เสียหายอีกด้วย ด้วยมาตรการต่าง ๆ ที่กล่าวข้างต้น จึงสามารถสรุปได้ว่าไม่มีช่องว่างของรูปแบบการกระทำผิดและมาตรการ

๕) มิจฉาชีพได้ใช้ Mobile Banking และบัญชีม้าในการโยกย้ายทรัพย์สิน ด้วยบัญชีม้าควบคู่กับ Mobile Banking ทำให้การโยกย้ายทรัพย์สินของมิจฉาชีพดำเนินการได้อย่างรวดเร็วและติดตามได้ยาก เมื่อมิจฉาชีพสามารถหลอกลวงผู้เสียหายได้สำเร็จ มิจฉาชีพจะใช้ Mobile Banking โยกย้ายเงินจากบัญชีม้าหนึ่งไปสู่อีกบัญชีม้าหนึ่งเพื่อนำเงินไปถึงมือของมิจฉาชีพให้เร็วที่สุด ในส่วนนี้ มาตรการหลักมักมาจาก ธปท. และสถาบันการเงิน โดย ธปท. ได้มีมาตรการหลายประการ

ในการลดช่องว่างของการใช้งาน Mobile Banking ที่มิจฉาชีพนำไปใช้ประโยชน์ได้ เช่น การต้องให้มีระบบการยืนยันตัวตนของผู้ใช้งาน การจำกัดวงเงินในการทำธุรกรรมทางการเงินในแต่ละครั้งและยอดรวมของแต่ละวัน เป็นต้น นอกจากนี้ ยังมีแนวทางเพื่อป้องกันการเปิดบัญชีม้าอีกด้วย เพราะฉะนั้น จึงกล่าวได้ว่ามีมาตรการหรือแนวทางในการรับมือกับการใช้ Mobile Banking แล้ว จึงไม่มีช่องว่างดังกล่าว

๖) เมื่อมีการหลอกลวงแล้ว ผู้เสียหายจะมีการแจ้งความร้องทุกข์และติดต่อหน่วยงานต่าง ๆ ที่เกี่ยวข้อง โดยเมื่อพิจารณาในเรื่องมาตรการและแนวทางในการรับมือต่าง ๆ นั้น ก็จะเห็นว่าหน่วยงานหลายแห่งได้มีช่องทางในการติดต่อรับเรื่องร้องเรียนแล้ว โดยเฉพาะสำนักงานตำรวจแห่งชาติและ บช.สอท. โดยเมื่อมีการแจ้งความร้องทุกข์ ก็จะมีการดำเนินคดีตามกฎหมายที่เกี่ยวข้อง โดยการดำเนินการได้รวมถึงการรวบรวมข้อมูลหลักฐานต่าง ๆ และข้อมูลของผู้กระทำผิด ซึ่งส่วนนี้ได้มีมาตรการในการเปิดเผยและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานแล้ว ตามที่กำหนดในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี นอกจากนี้ จากพระราชกำหนดดังกล่าว เมื่อมีความเสียหายเกิดขึ้นแล้ว เจ้าหน้าที่ตำรวจและเจ้าหน้าที่ที่เกี่ยวข้องมีอำนาจในการระงับธุรกรรมทางการเงินต้องสงสัยทุกทอด และอายัดบัญชีต้องสงสัยได้ ซึ่งเป็นการดำเนินการที่ช่วยเหลือผู้เสียหาย จึงนับว่ามีมาตรการแล้ว อย่างไรก็ดี พบว่ายังไม่มีมาตรการหรือแนวทางในการรับมือกับความเสียหายทางจิตใจหรือปัญหาสุขภาพจิตของผู้เสียหาย จึงสามารถนับเป็นช่องว่างที่ยังไม่มีการดำเนินการและควรมีการพิจารณาต่อไป

โดยสรุปแล้ว นอกจากเรื่องมาตรการรับมือกับความเสียหายของสุขภาพจิตของผู้เสียหาย ปัจจุบันได้มีแนวทางหรือมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงแล้วกล่าวคือมีได้มีช่องว่างของรูปแบบและพฤติกรรมของการหลอกลวงกับมาตรการของหน่วยงานต่าง ๆ อย่างไรก็ดี มาตรการแต่ละมาตรการอาจยังมีความไม่เหมาะสมกับการแก้ปัญหาหรือยังไม่เพียงพอที่จะทำให้สามารถบรรลุเป้าหมายของการแก้ไขและป้องกันปัญหาได้ ในส่วนต่อไป จะเป็นการวิเคราะห์มาตรการต่าง ๆ โดยละเอียดเพื่อหาช่องว่างของมาตรการปัจจุบันและมาตรการที่เหมาะสมตามเป้าหมายที่ตั้งไว้ โดยมุ่งเน้นไปที่องค์ประกอบหลัก ๓ ประการของการกระทำผิด ทั้งผู้กระทำผิด ผู้เสียหายและโอกาส เพื่อให้สามารถแก้ไขและป้องกันปัญหาได้อย่างครบถ้วน

แนวทางการดำเนินมาตรการเพื่อแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

จากลักษณะการกระทำผิดที่ได้อธิบายไปข้างต้นนั้น ในส่วนนี้จะเป็นการวิเคราะห์ช่องว่างของมาตรการแต่ละมาตรการตามการมุ่งเน้นไปที่แต่ละองค์ประกอบของการกระทำผิดตามทฤษฎีสามเหลี่ยมอาชญากรรม โดยจะมีการอธิบายถึงเป้าหมายในการแก้ไขและป้องกันปัญหาของแต่ละองค์ประกอบ จากนั้นจะเป็นการวิเคราะห์ช่องว่าง เพื่อให้เห็นช่องว่างของมาตรการที่มีอยู่กับมาตรการที่ควรเป็น และจะนำไปสู่สามารถมีการนำเสนอแนวทางในการปรับปรุงมาตรการที่มีอยู่ในปัจจุบันให้มีประสิทธิภาพมากยิ่งขึ้น ทั้งนี้นอกจากองค์ประกอบหลักทั้ง ๓ ประการตามทฤษฎีแล้ว ยังมีการวิเคราะห์และนำเสนอมาตรการที่เป็นการแก้ไขและป้องกันปัญหาในภาพรวมอีกด้วย

๑. เป้าหมายของการแก้ไขและป้องกันปัญหาการหลอกลวงในส่วนผู้กระทำผิด

เป้าหมายในการแก้ปัญหาในส่วนของผู้กระทำผิดประการแรกคือการสามารถจับกุมตัวผู้กระทำผิดได้ โดยการที่จะสามารถจับกุมผู้กระทำผิดได้จำเป็นต้องมีข้อมูลของผู้กระทำผิด ดังนั้น เมื่อมีความจำเป็นต้องใช้ข้อมูลเพื่อประโยชน์ของการสืบสวนสอบสวน หน่วยงานที่รับผิดชอบมีหน้าที่จะต้องให้ข้อมูลดังกล่าวอย่างครบถ้วนแก่เจ้าหน้าที่ที่เกี่ยวข้อง ในระยะเวลาอันรวดเร็ว เพื่อเป็นการเพิ่มโอกาสในการจับกุมผู้กระทำผิดได้มากขึ้น

เมื่อมีข้อมูลที่เพียงพอแล้ว ในการเข้าจับกุมผู้กระทำผิด มักพบว่าผู้กระทำผิดอาศัยอยู่ในต่างประเทศ โดยเฉพาะประเทศเพื่อนบ้าน สามารถกล่าวได้ว่าการหลอกลวงดังกล่าวมีลักษณะเหมือนองค์กรข้ามชาติ จึงต้องอาศัยความร่วมมือระหว่างประเทศ ดังนั้น การจับกุมจึงจำเป็นต้องมีการมีความร่วมมือระหว่างประเทศ โดยนอกจากการทำให้กระบวนการจับกุมดำเนินได้สะดวกขึ้นแล้ว ยังเป็นการสนับสนุนการดำเนินการปราบปรามและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์ในมิติอื่น ๆ ได้อีกด้วย

หลังจากจับกุมผู้กระทำผิดได้นั้น ก็ควรมีบทลงโทษผู้กระทำผิดที่ชัดเจน เหมาะสมแก่ความผิดและความเสียหาย ซึ่งนอกจากจะเป็นการลงโทษแล้ว ยังทำให้ผู้ที่คิดกระทำผิดเกิดความเกรงกลัวต่อการกระทำผิดได้

๒. เป้าหมายของการแก้ไขและป้องกันปัญหาการหลอกลวงในส่วนผู้เสียหาย

ตามที่ได้มีการอธิบายในบทที่ ๒ และบทที่ ๓ มิจฉาชีพมักใช้หลักการทางจิตวิทยาในการหลอกลวงเป้าหมาย ดังนั้น ในการแก้ปัญหาในส่วนของผู้เสียหายจึงเป็นการสร้างความตระหนักรู้แก่ประชาชน โดยมีการให้ความรู้แก่ประชาชนที่เหมาะสมเพียงพอ และอย่างทั่วถึงประชาชนทุกกลุ่ม

การสร้างความตระหนักรู้และให้ความรู้แก่ประชาชนนั้น ต้องดำเนินการควบคู่ไปกับการมีมาตรการคุ้มครองและปกป้องประชาชน เพราะการให้ความรู้เพียงอย่างเดียวนั้นยังไม่เพียงพอต่อการแก้ปัญหา โดยการปกป้องประชาชนจะประกอบด้วย การมีระบบแจ้งเตือนประชาชนเพื่อถูกมิจฉาชีพคุกคาม มีระบบแจ้งเตือนที่ทำให้ผู้ใช้บริการสามารถรับรู้ได้โดยง่ายว่าสายเรียกเข้าหรือข้อความสั้นที่ติดต่อเข้ามาเป็นมิจฉาชีพ เพื่อให้ประชาชนสามารถตัดสายที่สงสัยว่าเป็นมิจฉาชีพได้ก่อนการถูกหลอกลวง อย่างไรก็ดี แม้ว่าจะมีการช่วยแจ้งเตือน ก็มีโอกาสที่เป้าหมายจะเผลอรับสายและถูกหลอกลวงได้ จึงควรมีการแจ้งเตือนอีกครั้งเมื่อเป้าหมายกำลังจะมีการเสียทรัพย์สินให้กับมิจฉาชีพ โดยมีการแจ้งเตือนใน Mobile Banking อีกครั้งหนึ่ง

แม้ว่าจะมีการแจ้งเตือนแล้ว ก็มีโอกาสเช่นกันที่มิจฉาชีพจะสามารถหลอกลวงผู้เสียหายได้ เมื่อมีความเสียหายเกิดขึ้นแล้ว ในส่วนของมาตรการที่เกี่ยวข้องกับผู้เสียหายนั้นจึงควรมีระบบที่ผู้เสียหายสามารถร้องเรียนแจ้งความเสียหายเพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถดำเนินการติดตามผู้กระทำผิดและติดตามทรัพย์สินของผู้เสียหายคืนได้ โดยการดำเนินการควรมีความสะดวกรวดเร็ว ดำเนินการได้โดยไม่ยุ่งยาก นอกจากการช่วยเหลือด้านคดีความและการติดตามทรัพย์สินคืนแล้ว จากกรณีศึกษาในต่างประเทศ พบว่าผู้เสียหายจำนวนมากมีความเสียหายทางด้านจิตใจ และผู้คนรอบข้างของผู้เสียหายก็มีโอกาสที่จะได้รับผลกระทบทางจิตใจนี้ด้วย จึงควรมีศูนย์รับปรึกษาปัญหาทางด้านสุขภาพจิต เพื่อช่วยเยียวยาผู้เสียหายและผู้ที่ได้รับผลกระทบอย่างเหมาะสมด้วย

๓. เป้าหมายของการแก้ไขและป้องกันปัญหาการหลอกลวงในส่วนโอกาสและช่องทางในการกระทำผิด

ด้วยลักษณะของโอกาสในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ที่สามารถพิจารณาได้ว่าเป็นช่องทางในการเข้าถึงประชาชนของมิจฉาชีพ หรือการติดต่อหาเป้าหมายได้ ดังนั้น เป้าหมายของการแก้ไขและป้องกันปัญหาประการสำคัญคือการปิดกั้นโอกาสที่มิจฉาชีพจะสามารถติดต่อหรือเข้าถึงประชาชนได้ นอกจากโอกาสในการติดต่อหาเป้าหมายแล้ว ยังมีโอกาสในแง่ของการที่ผู้กระทำผิดสามารถได้รับทรัพย์สินของผู้เสียหายโดยใช้การโอนเงินผ่านบัญชีม้า ใช้ Mobile Banking ในการทำธุรกรรมทางการเงินอย่างรวดเร็ว ซึ่งโอกาสหรือช่องทางเหล่านี้เป็นสิ่งที่มิจฉาชีพได้วางแผนมาเป็นอย่างดี โดยใช้ช่องทางของการอำนวยความสะดวกให้แก่ผู้บริโภคของสถาบันการเงินต่าง ๆ ดังนั้นแล้ว จุดประสงค์อีกประการหนึ่งของมาตรการในการแก้ปัญหาส่วนของโอกาสคือการตัดช่องทางและเครื่องมือต่าง ๆ ที่มิจฉาชีพใช้ประกอบความผิดทั้งหมดด้วย

๔. เป้าหมายของการแก้ไขและป้องกันปัญหาการหลอกลวงในภาพรวม

ในส่วนนี้เป็นการนำเสนอแนวทางในการแก้ปัญหาในภาพรวมที่ครอบคลุมทั้ง ๓ องค์ประกอบ ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นปัญหาที่เกี่ยวข้องกับหน่วยงานหลายหน่วยงานทั้งภาครัฐและเอกชน และการจะสามารถแก้ปัญหาได้นั้น จำเป็นต้องอาศัยความร่วมมือของหน่วยงานทั้งหมดในลักษณะของการบูรณาการของหน่วยงานที่เกี่ยวข้อง ทั้งหน่วยงานที่มีหน้าที่รับผิดชอบโดยตรง หน่วยงานที่ได้รับผลกระทบ และหน่วยงานที่มีความเชี่ยวชาญในการแก้ปัญหาเฉพาะทาง โดยความร่วมมือนี้สามารถเสนอแนวทางในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ นอกจากการเสนอและกำหนดแนวทางแก้ไขปัญหาแล้ว ยังเป็นการผลักดันให้มีการนำมาตรการที่กำหนดขึ้นไปปฏิบัติจริงด้วย

จากจุดประสงค์หลักของการแก้ปัญหา และเป้าหมายของการแก้ปัญหาที่กำหนดไว้ในแต่ละองค์ประกอบของความผิด จึงได้วิเคราะห์ช่องว่าง หรือ Gap Analysis ระหว่างเป้าหมายที่วางไว้ (Desired state) และมาตรการที่ดำเนินการในปัจจุบัน (Current state) โดยสรุปรายละเอียดดังนี้

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
องค์ประกอบที่ ๑ ผู้กระทำผิด			
เป้าหมายที่ ๑ การสามารถจับกุมตัวผู้กระทำผิดได้			
๑.๑ เมื่อมีความจำเป็นต้องใช้ข้อมูลเพื่อประโยชน์ของการสืบสวนสอบสวน หน่วยงานที่รับผิดชอบมีหน้าที่จะต้องให้ข้อมูลดังกล่าวอย่างครบถ้วนแก่เจ้าหน้าที่ที่เกี่ยวข้อง ในระยะเวลาอันรวดเร็ว เพื่อเป็นการเพิ่มโอกาสในการจับกุมผู้กระทำผิดได้มากขึ้น	ปัจจุบันมีการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเพื่อกำหนดให้หน่วยงานที่รับผิดชอบมีหน้าที่ต้องเปิดเผยหรือแลกเปลี่ยนข้อมูลโดยทันที หรือตามที่ผู้สั่งร้องขอ เมื่อมีการร้องเรียนทางช่องทางต่าง ๆ เจ้าหน้าที่ตำรวจจะมีการขอข้อมูลจากแต่ละหน่วยงานที่รับผิดชอบ เช่น ผู้ให้บริการโทรศัพท์เคลื่อนที่ ผู้ให้บริการโทรคมนาคมอื่น ธนาคาร โดยหน่วยงานเหล่านี้มีหน้าที่ที่จะต้องสนับสนุนการสอบสวนของเจ้าหน้าที่ตำรวจ ผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่หน่วยงานต่าง ๆ เห็นชอบร่วมกัน	ปัจจุบันได้มีการกำหนดหน้าที่ในการเปิดเผยหรือแลกเปลี่ยนข้อมูลการให้บริการระหว่างหน่วยงานที่เกี่ยวข้องแล้ว อย่างไรก็ดี แม้ว่าจะมีการกำหนดว่าต้องมีการเปิดเผยหรือแลกเปลี่ยนข้อมูล แต่ยังไม่มีรายละเอียดของระบบหรือกระบวนการเปิดเผยข้อมูล	ควรมีการกำหนดให้ชัดเจนถึงระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลดังกล่าว โดยควรเป็นระบบหรือกระบวนการที่เจ้าหน้าที่ที่เกี่ยวข้องสามารถได้รับข้อมูลไปใช้ในการสืบสวนสอบสวนอย่างทันท่วงที และผู้ให้ข้อมูลก็สามารถดำเนินการได้ และมีขั้นตอนการดำเนินการที่รัดกุมเพื่อมิให้ข้อมูลส่วนตัวของประชาชนรั่วไหลได้ ในส่วนนี้อาจพิจารณาได้ว่าเป็นการนำมาตรการที่มีอยู่แล้วไปใช้ให้เกิดผลตามที่ตั้งไว้

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
๑.๒ การมีความร่วมมือระหว่างประเทศเพื่อสนับสนุนการดำเนินการปราบปรามและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์ ซึ่งการหลอกลวงดังกล่าวมีลักษณะเหมือนองค์กรข้ามชาติ จึงต้องอาศัยความร่วมมือระหว่างประเทศ	ในกรณีที่ผู้กระทำผิดอยู่ในต่างประเทศ เจ้าหน้าที่ตำรวจจะมีการดำเนินการประสานงานกับทางการในประเทศนั้น ๆ เพื่อเข้าจับกุม หรือมีการใช้กฎหมายว่าด้วยการส่งผู้ร้ายข้ามแดน	การใช้กฎหมายว่าด้วยการส่งผู้ร้ายข้ามแดนยังมีข้อจำกัด ทั้งในเรื่องกระบวนการดำเนินการที่ล่าช้าและมีเงื่อนไขที่ต้องเป็นไปตามข้อตกลง เช่น ลักษณะความผิดและโทษของความผิดนั้น ซึ่งเป็นอุปสรรคในการนำมาใช้เป็นเครื่องมือในการจับกุมผู้ร้ายที่กระทำความผิดจากในต่างประเทศ ปัจจุบันยังไม่มีการจัดทำความร่วมมืออื่น ๆ ที่เป็นทางการในระดับความร่วมมือระหว่างประเทศในประเด็นการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ จึงยังไม่มีแนวทางร่วมกันในการแก้ไขปัญหาดังกล่าว	สร้างความร่วมมือระหว่างประเทศอย่างเป็นทางการในรูปแบบต่าง ๆ ทั้งการสร้างความร่วมมือใหม่ เช่น การทำ Memorandum of Understandings (MoU) ในระดับทวิภาคี และพัฒนาจากความร่วมมือเดิมที่มีอยู่ เช่น กรอบความร่วมมือ Association of Southeast Asian Nations (ASEAN) โดยความร่วมมือระหว่างประเทศอาจเป็นทั้งความร่วมมือในการจับกุม การวางแนวทางในการป้องกันปัญหา รวมทั้งการนำเสนอวิธีการหรือเทคโนโลยีใหม่ ๆ ที่เป็นประโยชน์ต่อประเทศสมาชิก
เป้าหมายที่ ๒ มีบทลงโทษผู้กระทำผิดที่ชัดเจน			
มีบทลงโทษผู้กระทำผิดที่ชัดเจน เหมาะสมแก่ความผิดและความเสียหาย และทำให้มิจฉาชีพเกิดความเกรงกลัวต่อการกระทำผิด	การกระทำผิดฐานหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา เช่น มาตรา ๓๔๑ ที่กำหนดโทษจำคุกไม่	บทลงโทษอาจยังไม่เหมาะสมแก่ความผิดและระดับความเสียหาย นอกจากนี้ ยังพบว่า บทลงโทษของมิจฉาชีพมีบทลงโทษน้อยกว่ากลุ่ม	ควรมีการกำหนดอัตราโทษที่สูงขึ้น หรือให้มีความสอดคล้องกับการลงโทษกลุ่มสนับสนุนมิจฉาชีพที่กำหนดไว้ในพระราชกำหนดมาตรการป้องกันและ

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
	เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ	ผู้สนับสนุนมิจฉาชีพอย่างกลุ่มผู้ซื้อขายซิมม้าและบัญชีม้า	ปราบปรามอาชญากรรมทางเทคโนโลยีอย่างไรก็ดี ความผิดฐานฉ้อโกงมีความครอบคลุมหลากหลาย จึงอาจพิจารณาบทลงโทษการกระทำความผิดโดยหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ หรือความผิดของอาชญากรรมทางเทคโนโลยี โดยให้มีการกำหนดลักษณะรายละเอียดและมีบทลงโทษเป็นการเฉพาะ
	มีบทลงโทษผู้ให้การสนับสนุนมิจฉาชีพ เช่น ผู้ซื้อขายซิมม้าและบัญชีม้า ตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ดังนี้ ■ มาตรา ๙ ห้ามการให้ผู้อื่นใช้บัญชีของตน (บัญชีม้า) หรือซิมการ์ดที่ลงทะเบียนในชื่อของตน (ซิมม้า) โดยมีโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ	มีการกำหนดโทษที่ชัดเจนแล้ว	ไม่มี

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
	■ มาตรา ๑๐ และมาตรา ๑๑ ห้ามการจัดหาหรือซื้อขายบัญชีม้า และซิมม้า ตามลำดับ โดยมีโทษจำคุกตั้งแต่สองปีถึงห้าปี ปรับตั้งแต่สองแสนถึงห้าแสนบาท หรือทั้งจำทั้งปรับ		
องค์ประกอบที่ ๒ ผู้เสียหาย			
เป้าหมายที่ ๑ การสร้างความตระหนักรู้หรือการสร้างภูมิคุ้มกันแก่ประชาชน			
มีการให้ความรู้แก่ประชาชนที่เหมาะสมเพียงพอ และอย่างทั่วถึงประชาชนทุกกลุ่ม เพื่อให้มีความตระหนักรู้ มีความรู้ความเข้าใจ และมีการรับมือเมื่อถูกคุกคามโดยมิจฉาชีพได้ถูกต้อง ลดโอกาสการตกเป็นผู้เสียหาย โดยอาจพิจารณาการวัดผลด้วยวิธีการต่าง ๆ เพื่อให้มีการปรับปรุงวิธีการให้ความรู้	มีการจัดทำฐานข้อมูลที่เป็นแหล่งความรู้ให้แก่ประชาชน เช่น การจัดทำฐานข้อมูลชื่อ “SCAM Alert/เท่าทันมิจฉาชีพ” ของสำนักงาน กสทช. การจัดตั้งศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.) ที่เป็นแหล่งความรู้ที่ ธปท. จัดตั้งขึ้น การโฆษณาผ่านสื่อต่าง ๆ ของ บช. สอท. เป็นต้น นอกจากนี้ ธปท. ได้มีการให้ประชาชนทำแบบทดสอบเพื่อเพิ่มความตระหนักรู้ใน Mobile Banking หรือที่เรียกว่าการประเมินการ	แม้ว่าจะมีการให้ความรู้อย่างเหมาะสมและครบถ้วน รวบรวมไว้ในฐานข้อมูลต่าง ๆ แต่หากประชาชนมิได้มีการเข้าถึงฐานข้อมูลเหล่านั้น ก็อาจไม่ได้รับข้อมูลที่เพียงพอ นอกจากนี้ ยังมีกลุ่มประชาชนที่ยังขาดโอกาสในการเข้าถึงสื่อหรืออินเทอร์เน็ต ก็ทำให้ได้รับข้อมูลข่าวสารน้อยลงด้วย	ควรมีการใช้สื่อประชาสัมพันธ์ที่หลากหลายมากขึ้น โดยคำนึงถึงข้อจำกัดในการเข้าถึงสื่อของประชาชนทุกกลุ่ม เพื่อให้ข้อมูลถูกส่งต่อไปยังประชาชนให้มากที่สุด

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
	ตระหนักรู้ต่อภัยทุจริต (Awareness Test) เป็นระยะ ๆ		
เป้าหมายที่ ๒ การมีระบบแจ้งเตือนประชาชนเพื่อถูกมิจฉาชีพคุกคาม			
มีระบบแจ้งเตือนที่ทำให้ผู้ใช้บริการสามารถรับรู้ได้โดยง่ายว่าสายเรียกเข้าหรือข้อความสั้นที่ติดต่อเข้ามาเป็นมิจฉาชีพ โดยให้มีการปรากฏชื่อของผู้โทร (Sender name) โดยที่ประชาชนไม่จำเป็นต้องบันทึกเลขหมายนั้นไว้ในโทรศัพท์ของตนล่วงหน้า โดยเฉพาะหน่วยงานหรือองค์กรที่มักถูกมิจฉาชีพแอบอ้าง การมีระบบ Sender name ทำให้ประชาชนสามารถประเมินได้ทันทีว่าสายเรียกเข้านั้นมีโอกาสเป็นมิจฉาชีพมากน้อยเพียงใด นอกจากนี้ควรมีระบบตรวจสอบตัวตนของผู้โทร เพื่อป้องกันมิให้มีการปลอมแปลงเลขหมายหรือตัวตนของผู้โทร (Calling Line Identification:	ปัจจุบัน หน่วยงานที่เกี่ยวข้องได้มีระบบการแจ้งเตือนเมื่อมีการติดต่อจากมิจฉาชีพดังนี้ ■ การให้มี Sender name ของผู้ส่งข้อความสั้น (SMS) โดยเฉพาะชื่อขององค์กรหรือบริษัทที่มักถูกมิจฉาชีพนำไปแอบอ้าง ■ การเตือนผู้ใช้บริการเมื่อมีเลขหมายที่โทรมาจากต่างประเทศผ่าน VoIP โดยการใส่ Prefix “+๖๙๗” ซึ่งมิจฉาชีพมักใช้การโทรจากต่างประเทศเข้ามา จึงเป็นการเตือนให้ผู้ใช้ระมัดระวังสายเรียกเข้าที่มี Prefix ข้างต้น ■ การกำหนดให้ผู้ให้บริการโทรศัพท์ระหว่างประเทศ ผู้ให้บริการ	ปัจจุบันได้มีมาตรการแจ้งเตือนด้วยการปรากฏชื่อของผู้ส่ง (Sender name) ในบริการข้อความสั้นแล้ว แต่ยังไม่มีการใช้ Sender name ในการโทรด้วยเสียง แม้ว่าปัจจุบันได้มีการเติม Prefix ในเลขหมายจากต่างประเทศ แต่หากเป็นกรณีที่มิจฉาชีพโทรโดยใช้ Simbox เข้ามาช่วย ก็จะไม่มีการปรากฏ Prefix ดังกล่าว นอกจากนี้ แม้ว่าจะเป็นการแจ้งเตือนด้วย Prefix ก็ยังไม่ชัดเจนว่าเป็นมิจฉาชีพ ด้วยประชาชนบางส่วนยังต้องมีการติดต่อกับต่างประเทศ จึงอาจรับสายของมิจฉาชีพโดยไม่ทันระวังตัว จึงเป็นช่องว่างของมาตรการที่ควรปรับปรุงต่อไป	ควรมีการพิจารณานำระบบ Sender name มาใช้ในการโทรด้วยเสียง โดยอาศัยความร่วมมือระหว่างผู้ให้บริการโทรศัพท์เคลื่อนที่และหน่วยงานต่าง ๆ ในการมาลงทะเบียนเพื่อให้ได้ Sender name ของตนเอง อาจมีการพิจารณานำระบบตรวจสอบตัวตนของผู้โทรมาใช้ ดังที่มีตัวอย่างการใช้ในต่างประเทศ เช่น ระบบ CLI ของสหราชอาณาจักร หรือระบบ STIR/SHAKEN ของสหรัฐอเมริกา โดยกำหนดเป็นข้อบังคับที่ผู้ให้บริการโทรศัพท์เคลื่อนที่ต้องดำเนินการติดตั้งระบบดังกล่าวในเครือข่ายของตน โดยนอกจากการใช้ระบบดังกล่าวจะสามารถช่วยตรวจสอบตัวตนของผู้โทรแล้ว ยัง

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
CLI) ได้ และควรมีระบบการกรองเลขหมายหรือข้อความสั้นที่แม่นยำ โดยสามารถคัดแยกได้ว่าสายเรียกเข้าหรือข้อความใดเป็นมิจฉาชีพและจากบุคคลทั่วไป เพื่อมิให้ผู้ใช้บริการมีความเสี่ยงที่จะพลาดสายเรียกเข้าหรือข้อความที่สำคัญไป	Call Termination และผู้ให้บริการโทรศัพท์เคลื่อนที่จะต้องเพิ่ม Prefix สำหรับกรณีบริการที่ระบุเลขหมายต้นทางจากต่างประเทศ โดยใช้เครื่องหมาย “+๖๙๘” นำหน้าเลขหมายที่เป็น Roaming จากต่างประเทศ ■ สำนักงาน กสทช. มีการพัฒนาแอปพลิเคชัน “กันกวน” เพื่อแจ้งเตือนผู้ใช้บริการเมื่อมีเลขหมายที่คาดว่าเป็นมิจฉาชีพ โดยแอปพลิเคชันจะรวบรวมข้อมูลจากการรายงานของผู้ใช้บริการปัจจุบัน แอปพลิเคชันกันกวนอยู่ระหว่างการโอนย้ายไปอยู่ในความรับผิดชอบของสมาคมโทรคมนาคมแห่งประเทศไทย	ในส่วนของแอปพลิเคชัน ยังพบว่ามีความยุ่งยากในการต้องติดตั้งแอปพลิเคชันเสริม รวมทั้งแอปพลิเคชันอาจทำงานได้ไม่เต็มประสิทธิภาพเพราะต้องพึ่งพาข้อมูลที่ผู้ใช้งานร่วมกันแจ้งในแอปพลิเคชัน จึงไม่สามารถแจ้งเตือนผู้ใช้บริการในทุกสายของมิจฉาชีพได้	สามารถช่วยกรองเลขหมายที่เป็นเลขหมายของมิจฉาชีพโดยผู้ใช้บริการไม่จำเป็นต้องติดตั้งแอปพลิเคชันเพิ่มเติม
เป้าหมายที่ ๓ การมีระบบแจ้งเตือนประชาชนก่อนการโอนเงิน			
ให้มีการแจ้งเตือนบน Mobile Banking ทุกครั้งที่มีการทำธุรกรรม เนื่องจากเป็น	ธปท. ได้กำหนดให้ธนาคารต้องแจ้งเตือนบน mobile banking ก่อนทำธุรกรรมทุกครั้ง	มีการกำหนดมาตรการที่ชัดเจนแล้ว	ไม่มี

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
ช่องทางที่เป้าหมายจะสูญเสียทรัพย์สินให้แก่มิจฉาชีพได้			
เป้าหมายที่ ๔ การช่วยเหลือและเยียวยาผู้เสียหาย			
๔.๑ มีระบบที่ผู้เสียหายสามารถร้องเรียนแจ้งความเสียหายเพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถดำเนินการติดตามผู้กระทำผิดและติดตามทรัพย์สินของผู้เสียหายคืนได้ โดยการดำเนินการควรมีความสะดวก รวดเร็ว ดำเนินการได้โดยไม่ยุ่งยาก สามารถดำเนินการตลอด ๒๔ ชั่วโมง และเมื่อมีการร้องเรียนหรือแจ้งความร้องทุกข์แล้ว หน่วยงานที่เกี่ยวข้องรวมทั้งเจ้าหน้าที่ตำรวจ ต้องมีแนวทางและกรอบระยะเวลาการดำเนินที่ชัดเจน	มีการช่วยเหลือในเรื่องที่เกี่ยวข้องกับคดีความและการติดตามทรัพย์สิน โดยผู้เสียหายสามารถแจ้งความในพื้นที่ใดก็ได้ และยังสามารถแจ้งความออนไลน์ได้ที่ thaipoliceonline.com โดยพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้กำหนดขั้นตอนการดำเนินการที่เกี่ยวข้องการระงับธุรกรรมทางการเงินต้องสงสัยหลังจากมีการแจ้งความร้องทุกข์ไว้อย่างชัดเจน	มีการกำหนดมาตรการที่ชัดเจนในเรื่องการระงับธุรกรรมทางการเงินแล้ว แต่ยังไม่มีการกำหนดแนวทางการดำเนินการที่เกี่ยวข้องกับเลขหมายโทรศัพท์ที่ใช้ในการหลอกลวง เช่น การระงับเลขหมายไว้ชั่วคราว เมื่อมีการแจ้งความร้องทุกข์	อาจมีการพิจารณาในเรื่องการดำเนินการที่เกี่ยวข้องกับเลขหมายโทรศัพท์ที่มิจฉาชีพใช้ในการหลอกลวง อย่างไรก็ดี ประเด็นนี้อาจมีความเกี่ยวพันกับเรื่องของสิทธิและเสรีภาพของผู้ใช้บริการ โดยผู้ให้บริการโทรศัพท์เคลื่อนที่อาจไม่สามารถดำเนินการระงับสัญญาณโทรศัพท์ของเลขหมายนั้น ๆ ได้อย่างรวดเร็ว และอาจติดขัดในเรื่องปัญหาทางเทคนิค จึงเห็นควรให้มีการปรึกษาร่วมกันกับผู้ให้บริการโทรศัพท์เคลื่อนที่เพื่อให้มีแนวทางที่สามารถปฏิบัติได้จริง

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
๔.๒ เมื่อเกิดเหตุขึ้น ผู้เสียหายต้องสามารถติดต่อหน่วยงานที่เกี่ยวข้องได้อย่างสะดวก และรวดเร็วทันต่อเวลา โดยต้องเป็นช่องทางในการติดต่อสำหรับเรื่องการหลอกลวงหรืออาชญากรรมทางเทคโนโลยีโดยเฉพาะ เนื่องจากการดำเนินการที่รวดเร็วเป็นการเพิ่มโอกาสที่ผู้เสียหายจะได้ทรัพย์สินคืน นอกจากนี้ เจ้าหน้าที่ของหน่วยงานนั้น ๆ ต้องสามารถติดต่อประสานงานหน่วยงานที่เกี่ยวข้อง และให้ข้อมูลที่ถูกต้องแก่ผู้ร้องเรียนได้ โดยช่องทางการติดต่อหน่วยงานที่เกี่ยวข้องต้องมีการประชาสัมพันธ์ให้ประชาชนได้รับทราบโดยทั่วถึง	เมื่อเกิดเหตุขึ้นแล้ว ผู้เสียหายสามารถประสานงานไปยังหน่วยงานที่เกี่ยวข้องได้ เช่น ธนาคารที่ตนได้มีการทำธุรกรรม ซึ่ง ธปท. ได้กำหนดให้ทุกธนาคารมีช่องทางติดต่อเร่งด่วน (hotline) ตลอด ๒๔ ชั่วโมง และ ธปท. ยังมีศูนย์คุ้มครองผู้ใช้บริการทางการเงินของตนเอง (Call center ๑๒๑๓) นอกจากนี้ ยังมีศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์ (ศูนย์ ๑๒๑๒ ETDA) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อเชื่อมต่อข้อมูลเรื่องร้องเรียนการฉ้อโกงผ่านระบบโทรศัพท์เคลื่อนที่และสื่ออิเล็กทรอนิกส์	ปัจจุบัน หน่วยงานที่เกี่ยวข้องได้มีการตระหนักถึงปัญหาและจัดเตรียมช่องทางการติดต่อจากประชาชนหรือผู้ใช้บริการโดยให้เป็นช่องทางเฉพาะสำหรับเรื่องอาชญากรรมทางเทคโนโลยีเท่านั้นแล้ว อย่างไรก็ดี เนื่องจากเลขหมายที่ใช้ติดต่อหน่วยงานที่ต่าง ๆ ยังเป็นเลขหมายที่ต่างกัน อาจทำให้ประชาชนสับสน จึงอาจมีการพิจารณาช่องทางการติดต่อที่เป็นศูนย์กลางการติดต่อในเรื่องอาชญากรรมออนไลน์ให้มีความเป็นหนึ่งเดียวกัน และมีการประสานงานต่อไปตามแต่หน่วยงานที่รับผิดชอบ	อาจพิจารณาการใช้เลขหมายเดียวกันในลักษณะของศูนย์กลางในการติดต่อในเรื่องปัญหาอาชญากรรมทางเทคโนโลยี เพื่อไม่ให้เกิดความสับสนและประชาสัมพันธ์ให้ประชาชนรับทราบอย่างทั่วถึง
๔.๓ มีศูนย์เยียวยาและฟื้นฟูสุขภาพจิตของผู้เสียหายและผู้ที่เกี่ยวข้องกับผู้เสียหาย เนื่องจากการศึกษากรณีในต่างประเทศและเหตุที่เกิดขึ้นใน	- ยังไม่ชัดเจน -	ยังไม่มีการพิจารณาประเด็นเรื่องปัญหาสุขภาพจิตจากปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่	ควรมีการพิจารณาประเด็นเรื่องปัญหาสุขภาพจิตจากปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ เพื่อให้มีการจัดตั้งศูนย์เยียวยาและฟื้นฟูสุขภาพจิต

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
ประเทศไทย พบว่าผู้เสียหายจำนวนมากมีปัญหาสุขภาพจิตจากการถูกหลอกลวง ซึ่งนอกจากการช่วยเยียวยาและฟื้นฟูจิตใจ ยังให้คำแนะนำเพื่อให้ผู้เสียหายคลายความกังวลเมื่อต้องมีการให้ข้อมูลที่จำเป็นแก่เจ้าหน้าที่ตำรวจ ซึ่งข้อมูลเหล่านี้จะเป็นประโยชน์ต่อการแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ต่อไป			ของผู้เสียหายและผู้ที่เกี่ยวข้องกับผู้เสียหาย ซึ่งต้องมีเจ้าหน้าที่ที่มีความชำนาญเฉพาะทาง โดยประเด็นนี้ควรมีหน่วยงานที่มีความเชี่ยวชาญในเรื่องสุขภาพจิตเข้ามามีส่วนร่วม เช่น กรมสุขภาพจิต กระทรวงสาธารณสุข
องค์ประกอบที่ ๓ โอกาสและช่องทางของการกระทำผิด			
เป้าหมายที่ ๑ การปิดกั้นและจำกัดโอกาสการติดต่อเป้าหมายของผู้กระทำผิด			
๑.๑ มีมาตรการที่สามารถปิดกั้นและจำกัดโอกาสที่ผู้กระทำผิดหรือมิจฉาชีพสามารถติดต่อพูดคุยกับเป้าหมายได้ซึ่งมิจฉาชีพจะใช้โอกาสนี้หลอกลวงเป้าหมายด้วยเทคนิคทางจิตวิทยา อย่างไรก็ดี การปิดกั้นการโทรหรือข้อความสั้นจากมิจฉาชีพต้องมีระบบการคัดกรองที่มีประสิทธิภาพ โดยต้อง	การปิดกั้นการติดต่อจากมิจฉาชีพ ■ ปิดกั้น SMS และเบอร์ Call center ที่แอบอ้างเป็นธนาคาร และปิด website หลอกลวง ■ ระงับทราฟฟิคการโทรเข้าจากต่างประเทศมายังเลขหมายปลายทางของประเทศไทย ซึ่งมีรูปแบบของเลขหมายที่โทรเข้าเป็นรหัสโทรศัพท์ประจำ	นอกจากธนาคารแล้ว ยังไม่มีความชัดเจนในเรื่องการปิดกั้น SMS และเลขหมายที่แอบอ้างจากหน่วยงานอื่น ด้วยข้อจำกัดทางเทคนิคและกฎหมาย มาตรการในปัจจุบันจึงเป็นการระงับทราฟฟิคหรือสายเรียกเข้าแบบเหมารวมเป็นส่วนใหญ่ เช่น ระงับสายเรียกเข้าจากต่างประเทศทั้งหมด ซึ่งแม้จะ	ควรมีความร่วมมือระหว่างหน่วยงานที่มีความเกี่ยวข้องกับการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ รวมทั้งหน่วยงานที่ถูกแอบอ้างบ่อยครั้ง เพื่อให้มีการปิดกั้นเลขหมายที่แอบอ้างในลักษณะเดียวกันกับการแจ้งเตือนประชาชน คือควรมีการใช้ระบบคัดกรองเลขหมายที่คาดว่าเป็นมิจฉาชีพ

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
สามารถกรองสายที่เรียกเข้าหรือข้อความนั้นมาจากมิจฉาชีพหรือผู้ที่จำเป็นต้องติดต่อ	ประเทศ (Country Code) ที่ยังไม่ได้กำหนดโดย ITU ■ สำนักงาน กสทช. ได้มีจัดทำบริการ USSD (Unstructured Supplementary Services Data) หมายเลข *๑๓๘ เพื่อให้ผู้ใช้บริการสามารถเลือกปฏิเสธการรับสายที่เป็นทราฟฟิกจากต่างประเทศได้	เป็นการปกป้องประชาชนได้ดี แต่ก็มีข้อเสียจากการดำเนินการ เช่น อาจปิดกั้นสายที่จำเป็นต้องติดต่อออกไป	โดยใช้ระบบการตรวจสอบตัวตนของผู้โทร เพื่อให้มีการปิดกั้นเลขหมายของมิจฉาชีพได้
๑.๒ มีการตรวจสอบความผิดปกติของตรวจสอบทราฟฟิกการโทรเข้าจากต่างประเทศที่มีพฤติกรรมการใช้งานที่ผิดปกติ โดยไม่ต้องรอการร้องเรียนหรือแจ้งความร้องทุกข์จากผู้เสียหาย ซึ่งถือเป็นการวางมาตรการเชิงรุก เพื่อป้องกันไม่ให้มีการเสียหายเกิดขึ้น	ตรวจสอบความผิดปกติ โดยสำนักงาน กสทช. ได้มีการจัดทำมาตรการเชิงรุกโดยดำเนินการติดตามตรวจสอบทราฟฟิคการโทรเข้าจากต่างประเทศที่มีพฤติกรรมการใช้งานที่ผิดปกติ	มาตรการมีความเหมาะสมแล้ว	ไม่มี
๑.๓ ป้องกันมิให้ประชาชนหลงกลกดลิงก์ที่แฝงมัลแวร์ของมิจฉาชีพได้ โดยการประชาสัมพันธ์ห้ามประชาชนกดลิงก์ที่แนบมากับ SMS และอีเมล และ	ให้ธนาคารงดส่งลิงก์ทุกประเภทผ่าน SMS อีเมล และงดส่งลิงก์ขอข้อมูลสำคัญ	นอกจากธนาคารแล้ว ยังมีความไม่ชัดเจนว่าหน่วยงานที่เกี่ยวข้องอื่น ๆ มีมาตรการอย่างไร	หน่วยงานภาครัฐหรือเอกชนควรงดการส่งลิงก์ให้กับประชาชน เพื่อลดความเสี่ยงที่ประชาชนจะกดลิงก์ที่แอบอ้างโดยมิจฉาชีพ

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
ในขณะเดียวกัน ทางธนาคารก็มีนโยบายไม่มีส่งลิงก์ให้ผู้ใช้บริการโดยเด็ดขาดด้วย เพื่อให้ประชาชนไม่สับสน			
เป้าหมายที่ ๒ การปิดกั้นและจำกัดโอกาสช่องทางในการโยกย้ายทรัพย์สินของผู้กระทำผิด			
๒.๑ มีมาตรการที่รัดกุมโดยมิให้มีช่องว่างในการใช้งาน Mobile banking ที่มิจฉาชีพจะนำไปใช้ประโยชน์ได้	มีการป้องกันมิให้มีช่องว่างในการใช้งานบัญชีและ Mobile banking ที่ทำให้มิจฉาชีพนำไปใช้ในการหลอกลวงได้ ■ จำกัด ๑ บัญชีผู้ใช้งาน mobile banking (username) ของแต่ละธนาคาร ให้ใช้ได้ใน ๑ อุปกรณ์เท่านั้น ■ ธนาคารต้องให้ยืนยันตัวตนขั้นต่ำด้วย biometrics เมื่อเปิดบัญชีแบบ non-face-to-face หรือเมื่อเปลี่ยนวงเงิน หรือเมื่อโอนเงินจำนวนมาก ■ กำหนดเพดานวงเงินถอน/ โอนสูงสุดต่อวันให้เหมาะสมตามระดับความเสี่ยงของกลุ่มผู้ใช้บริการแต่ละประเภท	มาตรการมีความเหมาะสมแล้ว	ไม่มี

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
	■ ธนาคารต้องปรับปรุงระบบรักษาความปลอดภัยบน Mobile banking ให้ทันสมัย		
๒.๒ มีมาตรการในการระงับหรืออายัดบัญชีหรือธุรกรรมที่ต้องสงสัยได้อย่างทันท่วงที เพื่อเป็นการระงับการโอนเงินของมิจฉาชีพและเพิ่มโอกาสที่ผู้เสียหายจะได้เงินคืนด้วย	ตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เมื่อมีการร้องเรียน หรือมีเหตุอันควรสงสัยในธุรกรรมทางการเงิน สถาบันการเงินและผู้ประกอบธุรกิจผู้รับโอนทุกทอดจะต้องระงับการทำธุรกรรมดังกล่าวไว้ทันที	มาตรการดังกล่าวยังขาดการระงับบัญชีหรือธุรกรรมทุกทอดของเจ้าของบัญชีเดียวกัน	มาตรการนี้สามารถใช้ร่วมกับพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ ซึ่งจะเป็นการอายัดบัญชีของเจ้าของเดียวกันทั้งหมด จึงไม่มีประเด็นเพิ่มเติม
๒.๓ มีการติดตามและตรวจสอบความผิดปกติของการทำธุรกรรมที่คาดว่ามีความเกี่ยวข้องกับอาชญากรรมหรือการทุจริตได้ โดยไม่ต้องรอการร้องเรียนหรือแจ้งความร้องทุกข์จากผู้เสียหาย ซึ่งถือเป็นการวางมาตรการเชิงรุก เพื่อป้องกันไม่ให้มีการเสียหายเกิดขึ้น	ตรวจจับ/ติดตามบัญชี และธุรกรรมต้องสงสัย เพื่อแก้ไขจุดบกพร่องในเรื่องหากพบบัญชีผิดปกติแล้วสถาบันการเงินไม่สามารถอายัดได้ทันที และยังมีระบบติดตามแบบ Real time ด้วย	มาตรการมีความเหมาะสมแล้ว	ไม่มี

ตารางที่ ๔-๑ การวิเคราะห์ช่องว่างของมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (ต่อ)

เป้าหมายของมาตรการ (Desired State)	มาตรการ/แนวทางในปัจจุบัน (Current State)	ช่องว่างของมาตรการ (Gap)	แนวทางในการปรับปรุง (Remedies)
ภาพรวมของมาตรการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่			
เป้าหมาย การจัดตั้งความร่วมมือแบบบูรณาการ			
การมีความร่วมมือแบบบูรณาการระหว่างหน่วยงานที่เกี่ยวข้อง ทั้งหน่วยงานที่มีหน้าที่รับผิดชอบโดยตรง หน่วยงานที่ได้รับผลกระทบ และหน่วยงานที่มีความเชี่ยวชาญในการแก้ปัญหาเฉพาะทาง โดยความร่วมมือนี้สามารถเสนอแนวทางในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ นอกจากการเสนอและกำหนดแนวทางแก้ไขปัญหาแล้ว ยังเป็นหน่วยงานที่ผลักดันให้มีการนำมาตรการที่กำหนดขึ้นไปปฏิบัติจริงด้วย	พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ มีการกำหนดให้แต่งตั้งคณะกรรมการเพื่อกำหนดแนวทางในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีและให้ข้อเสนอแนะเกี่ยวกับเหตุอันควรสงสัยตามพระราชกำหนดนี้ รวมทั้งให้คำแนะนำและคำปรึกษาเกี่ยวกับการปฏิบัติงานของเจ้าหน้าที่รัฐและหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามพระราชกำหนดนี้	แม้ว่าพระราชกำหนดจะมีการกำหนดบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องหลายหน่วยงาน แต่ยังเป็นการกำหนดให้มีความร่วมมือของหน่วยงานที่มีหน้าที่รับผิดชอบโดยตรงในการสืบสวนสอบสวนเป็นหลัก โดยยังไม่มีความร่วมมือของหน่วยงานที่ได้รับผลกระทบอื่น ๆ	อาจมีการจัดตั้งความร่วมมืออื่น ๆ เพิ่มเสริมการจัดตั้งคณะกรรมการของพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ โดยอาจมีลักษณะแบบการจัดตั้งคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งโทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง ซึ่งเป็นคณะทำงานที่มีหน่วยงานที่เกี่ยวข้องและได้รับผลกระทบ และหน่วยงานที่มีความเชี่ยวชาญเฉพาะทาง เป็นต้น

ที่มา : ประมวลโดยผู้วิจัย

จากการวิเคราะห์ช่องว่างของมาตรการข้างต้น สามารถสรุปแนวทางในการแก้ปัญหาและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ ที่ยังต้องมีการดำเนินการเพิ่มเติมจากที่มีอยู่ในปัจจุบันได้ดังนี้

๑. ผู้กระทำผิด

๑.๑ เนื่องจากพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ได้มีการกำหนดให้หน่วยงานที่เกี่ยวข้องต้องมีการเปิดเผยหรือแลกเปลี่ยนข้อมูลแก่เจ้าหน้าที่ตำรวจเพื่อการสืบสวนสอบสวนแล้ว แนวทางที่ต้องมีการดำเนินการเพิ่มเติมคือการตกลงร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง เพื่อกำหนดแนวทางของการเปิดเผยหรือแลกเปลี่ยนข้อมูล โดยควรมีระบบหรือกระบวนการที่เจ้าหน้าที่ที่เกี่ยวข้องสามารถได้รับข้อมูลไปใช้ในการสืบสวนสอบสวนอย่างทันท่วงที และผู้ให้ข้อมูลก็สามารถดำเนินการได้ รวมทั้งมีขั้นตอนการดำเนินการที่รัดกุมเพื่อมิให้ข้อมูลส่วนตัวของประชาชนรั่วไหลได้

๑.๒ การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นปัญหาที่มีลักษณะคล้ายคลึงกับอาชญากรรมข้ามชาติ การจับกุมและการแก้ไขปัญหาจึงต้องอาศัยความร่วมมือระหว่างประเทศ ดังนั้น จึงต้องมีความร่วมมือระหว่างประเทศอย่างเป็นทางการในรูปแบบต่าง ๆ ทั้งการสร้างความร่วมมือใหม่ เช่น การทำ Memorandum of Understandings (MoU) หรือสนธิสัญญา (Treaty) ในระดับทวิภาคี และพัฒนาจากความร่วมมือเดิมที่มีอยู่ เช่น กรอบความร่วมมือ Association of Southeast Asian Nations (ASEAN) โดยความร่วมมือระหว่างประเทศอาจเป็นทั้งความร่วมมือในการจับกุม การวางแนวทางในการป้องกันปัญหา รวมทั้งการนำเสนอวิธีการหรือเทคโนโลยีใหม่ ๆ ที่เป็นประโยชน์ต่อประเทศสมาชิก

๑.๓ บทลงโทษผู้กระทำผิดในปัจจุบันโดยหลักคือความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา โดยพบว่าบทลงโทษค่อนข้างน้อยเมื่อเทียบกับความผิดและความเสียหาย อีกทั้งยังมีบทลงโทษที่น้อยกว่ากลุ่มผู้ซื้อขายบัญชีและซิมม้า จึงควรมีการกำหนดอัตราโทษของผู้กระทำผิดที่สูงขึ้น หรือให้มีความสอดคล้องกับการลงโทษกลุ่มสนับสนุนมิจฉาชีพที่กำหนดไว้ในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี อย่างไรก็ดี ความผิดฐานฉ้อโกงมีความครอบคลุมหลากหลาย จึงอาจพิจารณาบทลงโทษการกระทำความผิดโดยหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ หรือความผิดของอาชญากรรมทางเทคโนโลยี โดยให้มีการกำหนดลักษณะรายละเอียดและมีบทลงโทษเป็นการเฉพาะ

๒. ผู้เสียหาย

๒.๑ การแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ที่สำคัญประการหนึ่งคือการสร้างความตระหนักรู้และให้ความรู้แก่ประชาชน เพื่อมิให้ตกเป็นผู้เสียหายได้ อย่างไรก็ดี พบว่าการประชาสัมพันธ์หรือให้ข้อมูลแก่ประชาชนผ่านสื่อต่าง ๆ อาจยังไม่เพียงพอด้วยประชาชนบางกลุ่มยังขาดโอกาสในการเข้าถึงสื่อ จึงควรมีการใช้สื่อประชาสัมพันธ์ที่หลากหลายมากขึ้น โดยคำนึงถึงข้อจำกัดในการเข้าถึงสื่อของประชาชนทุกกลุ่ม เพื่อให้ข้อมูลถูกส่งต่อไปยังประชาชนให้มากที่สุด

๒.๒ นอกจากการสร้างความตระหนักรู้แล้ว ควรมีมาตรการป้องกันหรือปกป้องประชาชนจากการเข้าถึงของมิจฉาชีพ เพื่อลดโอกาสที่ประชาชนจะถูกหลอกได้ โดยการป้องกันประการแรกคือการแจ้งเตือนให้ประชาชนทราบเมื่อมีการติดต่อจากมิจฉาชีพ เช่น ควรมีการพิจารณานำระบบ Sender name มาใช้ในการโทรด้วยเสียง โดยอาศัยความร่วมมือระหว่างผู้ให้บริการโทรศัพท์เคลื่อนที่และหน่วยงานต่าง ๆ ในการมาลงทะเบียนเพื่อให้ได้ Sender name ของตนเอง และอาจมีการพิจารณานำระบบตรวจสอบตัวตนของผู้โทรมาใช้ ดังที่มีตัวอย่างการใช้ในต่างประเทศ เช่น ระบบ CLI ของสหราชอาณาจักร หรือระบบ STIR/SHAKEN ของสหรัฐอเมริกา โดยกำหนดเป็นข้อบังคับที่ผู้ให้บริการโทรศัพท์เคลื่อนที่ต้องดำเนินการติดตั้งระบบดังกล่าวในเครือข่ายของตน โดยนอกจากการใช้ระบบดังกล่าวจะสามารถช่วยตรวจสอบตัวตนของผู้โทรแล้ว ยังสามารถช่วยกรองเลขหมายที่เป็นเลขหมายของมิจฉาชีพโดยผู้ใช้บริการไม่จำเป็นต้องติดตั้งแอปพลิเคชันเพิ่มเติม

๒.๓ ควรมีระบบการช่วยเหลือผู้เสียหาย ปัจจุบัน เมื่อมีการแจ้งความร้องทุกข์แล้วจะมีการระงับธุรกรรมทางการเงินต้องสงสัยและการอายัดบัญชีตามที่มีการกำหนดไว้ในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี อย่างไรก็ดี พบว่ายังไม่มีการดำเนินการระงับสัญญาณโทรศัพท์เมื่อมีการแจ้งความร้องทุกข์ จึงอาจมีการพิจารณาในเรื่องการดำเนินการที่เกี่ยวข้องกับเลขหมายโทรศัพท์ที่มิจฉาชีพใช้ในการหลอกลวง โดยประเด็นนี้อาจมีความเกี่ยวพันกับเรื่องของสิทธิและเสรีภาพของผู้ใช้บริการ โดยผู้ให้บริการโทรศัพท์เคลื่อนที่อาจไม่สามารถดำเนินการระงับสัญญาณโทรศัพท์ของเลขหมายนั้น ๆ ได้อย่างรวดเร็ว และอาจติดขัดในเรื่องปัญหาทางเทคนิค จึงเห็นควรให้มีการปรึกษาร่วมกันกับผู้ให้บริการโทรศัพท์เคลื่อนที่เพื่อให้มีแนวทางที่สามารถปฏิบัติได้จริง

๒.๔ ในการช่วยเหลือผู้เสียหายนั้น ควรต้องมีช่องทางในการติดต่อหน่วยงานที่เกี่ยวข้องที่รวดเร็วเพื่อให้มีความช่วยเหลือที่ทันท่วงทีได้ โดยในปัจจุบันได้มีช่องทางมากมายจากหลายหน่วยงาน แต่พบว่าแต่ละหน่วยงานต่างก็มีช่องทางการติดต่อของตัวเอง จึงอาจพิจารณาการใช้เลขหมายเดียวกันหรือมีช่องทางในลักษณะของศูนย์กลางในการติดต่อเฉพาะเรื่องปัญหาอาชญากรรมทางเทคโนโลยี เพื่อไม่ให้ประชาชนเกิดความสับสน และควรมีประชาสัมพันธ์ให้ประชาชนรับทราบอย่างทั่วถึง

๒.๕ ควรมีการพิจารณาประเด็นเรื่องปัญหาสุขภาพจิตของผู้เสียหายจากการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ เพื่อให้มีการจัดตั้งศูนย์เยียวยาและฟื้นฟูสุขภาพจิตของผู้เสียหายและผู้ที่เกี่ยวข้องกับผู้เสียหาย ซึ่งต้องมีเจ้าหน้าที่ที่มีความชำนาญเฉพาะทาง โดยประเด็นนี้ควรมีหน่วยงานที่มีความเชี่ยวชาญในเรื่องสุขภาพจิตเข้ามามีส่วนร่วม เช่น กรมสุขภาพจิต กระทรวงสาธารณสุข

๓. โอกาสและช่องทางของการกระทำผิด

๓.๑ มาตรการประการแรกคือการต้องมีการปิดกั้นหรือลดโอกาสที่มิจฉาชีพจะเข้าถึงประชาชนได้ เช่น การปิดกั้นเลขหมายที่ถูกแอบอ้างโดยมิจฉาชีพมิให้สามารถติดต่อประชาชนได้ ซึ่งการดำเนินการต้องอาศัยความร่วมมือระหว่างหน่วยงานที่มีความเกี่ยวข้อง โดยเฉพาะหน่วยงานที่ถูกแอบอ้างบ่อยครั้ง เพื่อให้มีการปิดกั้นเลขหมายที่แอบอ้าง ในลักษณะเดียวกันกับการแจ้งเตือน

ประชาชน คือควรมีการใช้ระบบคัดกรองเลขหมายที่คาดว่าเป็นมิจฉาชีพโดยใช้ระบบการตรวจสอบตัวตนของผู้โทร เพื่อให้มีการปิดกั้นเลขหมายของมิจฉาชีพได้

๓.๒ หน่วยงานภาครัฐหรือเอกชนควรงดการส่งลิงก์ให้กับประชาชน เพื่อลดความเสี่ยงที่ประชาชนจะกดลิงก์ที่แอบอ้างโดยมิจฉาชีพ โดยให้เป็นแนวปฏิบัติเดียวกัน เพื่อป้องกันความสับสนของประชนได้

๔. ภาพรวมของมาตรการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

อาจมีการจัดตั้งความร่วมมืออื่น ๆ เพิ่มเสริมการจัดตั้งคณะกรรมการของพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ โดยต้องมีลักษณะเป็นการบูรณาการของภาคส่วนต่าง ๆ ทั้งภาครัฐและเอกชน โดยอาจใช้ตัวอย่างการดำเนินการที่ผ่านมาเป็นแนวทางเบื้องต้น เช่น การจัดตั้งคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งโทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง ความร่วมมือนี้ควรเป็นการร่วมมือของหน่วยงานที่เกี่ยวข้องและได้รับผลกระทบ และหน่วยงานที่มีความเชี่ยวชาญเฉพาะทาง เพื่อให้มีการแก้ไขปัญหา นำเสนอมาตรการ และสามารถนำไปปฏิบัติให้เห็นผลได้

สรุป

ปัจจุบันหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนได้มีมาตรการหรือแนวทางในการแก้ปัญหาและป้องกันการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มากมาย โดยมุ่งเน้นทั้งในส่วนของผู้กระทำผิด ผู้เสียหาย และโอกาสหรือช่องทางของการกระทำผิด ซึ่งเป็นองค์ประกอบสำคัญของอาชญากรรมตามทฤษฎีสามเหลี่ยมอาชญากรรม จากการวิเคราะห์โดยใช้วิธีวิเคราะห์ช่องว่าง (Gap Analysis) ระหว่างรูปแบบหรือพฤติกรรมการหลอกลวงกับมาตรการหรือแนวทางในการแก้ไขและป้องกันปัญหาในปัจจุบัน พบว่ามีมาตรการแต่ละพฤติกรรมการกระทำผิดแล้ว ทว่า เมื่อมีการวิเคราะห์ในเรื่องมาตรการที่มีอยู่กับมาตรการที่เหมาะสมตามเป้าหมาย พบว่ายังมีส่วนต่างหรือช่องว่าง (Gap) ของมาตรการที่มีอยู่ในปัจจุบันและเป้าหมายของมาตรการ งานศึกษานี้จึงเสนอมาตรการหรือแนวทางเพิ่มเติมโดยคำนึงถึงการร่วมมือกันระหว่างหน่วยงานต่าง ๆ แบบบูรณาการ เพื่อให้สามารถแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ทั้งการดำเนินการให้สามารถจับกุมผู้กระทำผิดได้ โดยให้มีความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทั้งหมดในเรื่องระบบการเปิดเผยและแลกเปลี่ยนข้อมูล และการร่วมมือระหว่างประเทศเพื่อการจับกุมผู้กระทำผิดในต่างประเทศได้ การเพิ่มอัตราโทษของผู้กระทำผิดที่ยังมีความไม่สอดคล้องกับความเสียหายและการกำหนดโทษในกฎหมายอื่นที่เกี่ยวข้อง การสร้างความตระหนักรู้ให้แก่ประชาชนและมีแนวทางช่วยเหลือผู้เสียหายทั้งในเรื่องคดีความและการเยียวยาฟื้นฟูด้านสุขภาพจิต การนำเทคโนโลยีมาใช้เพื่อปิดกั้นโอกาสที่มิจฉาชีพจะสามารถติดต่อประชาชนได้ และประการสุดท้ายคือการจัดตั้งความร่วมมือระหว่างหน่วยงานอย่างเป็นทางการ เพื่อให้เกิดการแก้ปัญหาร่วมกันแบบบูรณาการ

บทที่ ๕
สรุปและข้อเสนอแนะ

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่โดยเฉพาะอย่างยิ่งภัยการหลอกลวงทางโทรศัพท์มิจฉาชีพคอลเซ็นเตอร์ หรือแก๊งคอลเซ็นเตอร์ (Call Center) ถือเป็นอาชญากรรมทางสังคมร้ายแรงในปัจจุบันซึ่งส่งผลกระทบกับประชาชนในวงกว้างและกระทบต่อความมั่นคงของประเทศอย่างมีนัยสำคัญ ซึ่งปัญหาดังกล่าวจำเป็นต้องมีการศึกษาเพื่อให้สามารถแก้ไขและป้องกันปัญหาได้ ในงานศึกษาเรื่อง “ข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ” จึงได้มีจุดประสงค์การวิจัยที่สำคัญ ๓ ข้อ ดังนี้

วัตถุประสงค์การวิจัยข้อที่ ๑ เพื่อศึกษาพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ และผลกระทบที่เกิดขึ้นต่อสังคมและผู้บริโภค

วัตถุประสงค์การวิจัยข้อที่ ๒ เพื่อศึกษาแนวทางการดำเนินการในการแก้ไขหรือป้องกันการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในปัจจุบัน

วัตถุประสงค์การวิจัยข้อที่ ๓ เพื่อนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

จากการศึกษาด้วยใช้ข้อมูลทั้งปฐมภูมิและทุติยภูมิ ทั้งการสัมภาษณ์กับผู้ที่เกี่ยวข้องกับปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ทั้งภาครัฐและเอกชน เช่น หน่วยงานกำกับดูแลด้านโทรคมนาคมและการเงินการธนาคาร เจ้าหน้าที่ตำรวจ และผู้ให้บริการโทรศัพท์เคลื่อนที่ การทบทวนวรรณกรรมและงานศึกษาที่เกี่ยวข้อง การค้นคว้าจากกรณีศึกษาต่างประเทศ เมื่อได้รับข้อมูลที่มีความครบถ้วนแล้วก็ได้ทำการวิเคราะห์ข้อมูลด้วยวิธีการเชิงคุณภาพ (Qualitative methodology) เช่น การวิเคราะห์ช่องว่าง (Gap Analysis) ระหว่างการรูปแบบพฤติกรรมการหลอกลวงและแนวทางหรือมาตรการในการแก้ไขและป้องกันปัญหาในปัจจุบัน รวมถึงการวิเคราะห์ช่องว่างระหว่างการดำเนินการในปัจจุบันและการดำเนินการที่สามารถต่อยอดได้เพื่อให้มีการแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่แบบบูรณาการให้มีประสิทธิภาพมากขึ้น นอกจากนี้ ยังมีการวิเคราะห์โดยใช้ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) เป็นหลัก ทฤษฎีดังกล่าวเป็นพื้นฐานในการอธิบายและวิเคราะห์องค์ประกอบต่าง ๆ ในการกระทำผิด รวมไปถึงการเสนอแนะแนวทางในการแก้ไขปัญหาอีกด้วย โดยผลการศึกษาตามแต่ละจุดประสงค์การวิจัย มีรายละเอียดดังนี้

สรุป

๑. ลักษณะสำคัญของพฤติกรรมการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

๑.๑ มิจฉาชีพมีการทำงานเป็นกลุ่มขบวนการ หรือที่เรียกว่าเป็น “แก๊ง” และมีการแบ่งงานกันทำ

จากการศึกษาพบว่า มิจฉาชีพมิได้มีเพียงผู้ที่ทำหน้าที่ติดต่อและหลอกลวงเป้าหมายเท่านั้น หากแต่ยังมีมิจฉาชีพคนอื่น ๆ ร่วมด้วย โดยมีการทำงานกันเป็นขบวนการและแบ่งหน้าที่กันทำอย่างชัดเจน หรือที่เรียกว่าเป็น “แก๊ง” โดยทั่วไปแล้ว ขบวนการดังกล่าวจะประกอบด้วยมิจฉาชีพ ๓ กลุ่มหลัก คือ (๑) มิจฉาชีพที่ทำหน้าที่ติดต่อเป้าหมาย ซึ่งทำหน้าที่เป็นหน้าด่านพูดคุยกับเป้าหมาย และหลอกล่อด้วยวิธีการทางจิตวิทยาต่าง ๆ เพื่อให้เป้าหมายหลงกลและยอมโอนเงินให้กับมิจฉาชีพ มิจฉาชีพกลุ่มนี้มักเป็นคนไทย เนื่องจากต้องมีทักษะในการสื่อสารกับคนไทยซึ่งเป็นกลุ่มเป้าหมายหลัก (๒) กลุ่มสนับสนุนหรือผู้ดูแลระบบ มิจฉาชีพกลุ่มนี้เป็นกลุ่มที่มิได้ติดต่อพูดคุยกับเป้าหมายโดยตรง แต่เป็นผู้ดำเนินการจัดหาทรัพยากร เตรียมอุปกรณ์ที่จำเป็น อำนวยความสะดวกต่าง ๆ ให้กับมิจฉาชีพกลุ่มแรก (๓) นายทุน เป็นผู้ที่ทำหน้าที่สนับสนุนค่าใช้จ่ายต่าง ๆ ที่เกิดขึ้น เช่น ค่าจ้างแรงงาน ค่าใช้จ่ายในอุปกรณ์ที่จำเป็น ค่าเช่าสถานที่ในการตั้งฐานปฏิบัติการ เป็นต้น

ขบวนการมิจฉาชีพหรือผู้กระทำผิดในความผิดการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่อาจพิจารณาได้ว่ามีลักษณะคล้ายกับองค์กรหรือบริษัทหนึ่ง และยังมีลักษณะคล้ายคลึงกับ “แฟรนไชส์” (Franchise) อีกด้วย ขบวนการมิจฉาชีพมีการทำงานที่เป็นระบบ มีการฝึกสอนแนวทางปฏิบัติให้กับมิจฉาชีพในกลุ่มทุกคน มีสูตรหรือคู่มือสำหรับใช้ในการหลอกลวง มีการศึกษาตลาดเป็นอย่างดีเพื่อให้ทันต่อสถานการณ์ มีการหาข้อมูลอย่างสม่ำเสมอ มีการวางระบบโยกย้ายเงินเพื่อให้ติดตามจับกุมได้ยาก เป็นต้น

๑.๒ มิจฉาชีพมีการตั้งฐานปฏิบัติการในต่างประเทศและมีลักษณะเหมือนอาชญากรรมข้ามชาติ

เนื่องจากกฎหมายไทยไม่สามารถบังคับใช้นอกราชอาณาจักร มิจฉาชีพจึงใช้ช่องว่างในส่วนนี้เพื่อหลีกเลี่ยงการจับกุม โดยมิจฉาชีพจะตั้งฐานปฏิบัติการในต่างประเทศ โดยเฉพาะในบริเวณชายแดนประเทศเพื่อนบ้านของไทย ซึ่งนอกจากจะทำให้การจับกุมผู้กระทำผิดทำได้ยากแล้ว ยังมีข้อดีอื่น ๆ ที่เป็นประโยชน์แก่มิจฉาชีพอีกด้วย เช่น บริเวณชายแดนไทยกับประเทศเพื่อนบ้านยังเป็นบริเวณที่สัญญาณโทรศัพท์เคลื่อนที่ของไทยยังสามารถใช้การได้ อีกทั้งสามารถขนย้ายแรงงานจากไทยเข้าไปได้สะดวก เป็นต้น นอกจากการตั้งฐานปฏิบัติการนอกประเทศที่เป็นเป้าหมายแล้ว ขบวนการมิจฉาชีพก็ใช้ได้แรงงานจากหลายประเทศร่วมในขบวนการดังกล่าว ทั้งการใช้คนไทยเป็นคนติดต่อเพื่อหลอกลวงเป้าหมายที่อาศัยอยู่ในประเทศไทย ใช้แรงงานท้องถิ่นในการจัดหาทรัพยากรที่จำเป็น โดยผู้ออกทุนอาจเป็นชาวต่างชาติรวมถึงชาวจีน ด้วยลักษณะดังกล่าวข้างต้น จึงกล่าวได้ว่าการทำงานของแก๊งคอลเซ็นเตอร์มีลักษณะเหมือนอาชญากรรมข้ามชาติ

๑.๓ มิจฉาชีพสามารถจัดหาช่องทางและอุปกรณ์ต่าง ๆ ที่ใช้ในการสื่อสารเพื่อเข้าถึงเป้าหมายได้หลายวิธี รวมทั้งการจัดหาซิมการ์ดหรือซิมม้า

ในการเข้าถึงเป้าหมายได้นั้น มิจฉาชีพมักใช้การโทรด้วยเสียงผ่านเครือข่ายโทรศัพท์ไปยังเป้าหมาย และมีบางกรณีที่ใช้การส่งข้อความสั้น อย่างไรก็ดี การใช้เลขหมายโทรศัพท์อาจทำให้เจ้าหน้าที่ตำรวจสามารถสืบทราบตัวตนของผู้กระทำผิดได้ เพราะปัจจุบันสำนักงาน กสทช. ได้มีการกำกับดูแลโดยให้ผู้ใช้งานเลขหมายทุกรายต้องลงทะเบียนเลขหมายกับผู้ให้บริการโทรศัพท์เคลื่อนที่ ซึ่งผู้ใช้บริการสามารถลงทะเบียนเลขหมายได้ด้วยตนเองและที่ลูกตู้ไม่เกินคนละ ๕ ซิม ด้วยข้อจำกัดนี้ มิจฉาชีพจึงต้องมีวิธีการในการได้มาซึ่งเลขหมายจำนวนมากและต้องเป็นเลขหมายที่ลงทะเบียนด้วยชื่อของผู้อื่น หรือที่เรียกว่าซิมม้า มิจฉาชีพได้มีการใช้ซิมม้าเป็นจำนวนมาก อย่างไรก็ดี เมื่อมีการปราบปรามการใช้ซิมม้าร่วมกับการปิดกั้นการโทรเข้าจากเลขหมายที่มีต้นทางอยู่ในต่างประเทศ มิจฉาชีพจึงปรับตัวไปใช้เทคโนโลยีอื่น ๆ ร่วมด้วย เช่น การใช้ Simbox จึงสามารถกล่าวได้ว่าพฤติกรรมของมิจฉาชีพจะมีการจัดหาช่องทางในการเข้าถึงเป้าหมายได้หลากหลายวิธี และสามารถปรับตัวได้อย่างรวดเร็ว

๑.๔ มิจฉาชีพได้ใช้หลักการหลอกลวงทางจิตวิทยาต่าง ๆ เพื่อโจมตีจุดอ่อนของเป้าหมาย

เมื่อสามารถเข้าถึงเป้าหมายได้แล้ว มิจฉาชีพจะใช้วิธีการทางจิตวิทยาในการโน้มน้าวเป้าหมายให้หลงเชื่อและยอมเสียทรัพย์ในที่สุด โดยหลักการที่มิจฉาชีพใช้ในการหลอกลวงประกอบด้วย ๘ หลักการ ซึ่งการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยมีการใช้โดยหลักการดังกล่าวในปริมาณมากน้อยแตกต่างกัน ตัวอย่างของพฤติกรรมการหลอกลวงที่พบได้บ่อยซึ่งตรงกับหลักการทางจิตวิทยาต่าง ๆ เช่น การแอบอ้างเป็นเจ้าหน้าที่รัฐหรือองค์กรต่าง ๆ ให้มีความน่าเชื่อถือ ซึ่งเป็นไปตามหลักการการปฏิบัติตามเงื่อนไขของสังคม (Social Compliance Principle) ซึ่งใช้ความเชื่อถือต่อองค์กรต่าง ๆ ในฐานะหน่วยงานที่มีอำนาจ (Authority) เป็นเครื่องมือ การแอบอ้างเป็นเจ้าหน้าที่ตำรวจและข่มขู่เป้าหมายด้วยคดีร้ายแรงเพื่อให้เป้าหมายเกิดความหวาดกลัว ซึ่งเป็นไปตามหลักการตอบสนองตามต้องการพื้นฐานของมนุษย์ (Visceral triggers) ซึ่งเป็นหลักการที่ใช้ความรู้สึกและความต้องการพื้นฐานของมนุษย์เป็นตัวหลอกล่อ การแอบอ้างเป็นเพื่อนเพื่อให้เป้าหมายเกิดความไว้ใจและขอยืมเงิน ซึ่งเป็นไปตามหลักการความใจดี (Kindness Principle) และการหลอกลวงมักบีบบังคับให้เป้าหมายต้องตัดสินใจในเวลาที่จำกัดเพื่อให้เป้าหมายตัดสินใจพลาดได้ง่าย ซึ่งเป็นไปตามหลักการด้านเวลา (Time Principle) โดยหลักการทางจิตวิทยาที่มิจฉาชีพใช้เหล่านี้มักมุ่งเน้นไปที่จุดอ่อนของมนุษย์ ทำให้เกิดความผิดพลาดในระบบการตัดสินใจ (Error in judgement) ของเป้าหมายได้ ปรากฏการณ์นี้สามารถเกิดขึ้นได้ในมนุษย์ทุกคน โดยเฉพาะกลุ่มคนที่พิจารณาได้ว่าขาดบางสิ่งในชีวิตมากกว่าคนทั่วไป เช่น ขาดความรัก ขาดการยอมรับจากสังคม รวมทั้งขาดเงินหรือปัจจัยพื้นฐานในการดำรงชีวิต ซึ่งกลุ่มเหล่านี้จะมีโอกาสตกเป็นผู้เสียหายได้สูงขึ้น

๑.๕ มิจฉาชีพใช้ Mobile Banking และบัญชีม้าในการโยกย้ายทรัพย์สิน

ช่องทางในการรับเงินจากผู้เสียหายคือการโอนเงินผ่านบัญชีธนาคาร บัญชีธนาคารจึงเป็นเครื่องมือที่สำคัญมากของกลุ่มมิจฉาชีพ ในลักษณะคล้ายกันกับการใช้ซิมม้า มิจฉาชีพก็มีการใช้บัญชีม้าหรือบัญชีที่เจ้าของบัญชีมิใช้ผู้รับเงินหรือมิใช่กลุ่มมิจฉาชีพเพื่อปกปิดตัวตนของ

มิจฉาชีพ โดยมักใช้บัญชีม้าควบคู่กับ Mobile Banking ซึ่งทำให้การโยกย้ายทรัพย์สินของมิจฉาชีพดำเนินการได้อย่างรวดเร็วและติดตามได้ยาก ซึ่งเป็นการใช้โอกาสที่สถาบันการเงินอำนวยความสะดวกผู้ใช้บริการให้เป็นประโยชน์ เมื่อมิจฉาชีพสามารถหลอกลวงผู้เสียหายได้สำเร็จ มิจฉาชีพจะใช้ Mobile Banking โยกย้ายเงินจากบัญชีม้าหนึ่งไปสู่อีกบัญชีม้าหนึ่งเพื่อนำเงินไปถึงมือของมิจฉาชีพให้เร็วที่สุด โดยบัญชีม้านี้มีหลายแถว กล่าวคือมีการเปลี่ยนสลับบัญชีม้าหลายบัญชี และปลายทางของบัญชีมักมีการแปลงให้สินทรัพย์อยู่ในรูปแบบเงินสกุลดิจิทัล ซึ่งทำให้ตรวจสอบและติดตามได้ยาก

เมื่อเป้าหมายหรือผู้เสียหายได้เสียทรัพย์สินให้กับมิจฉาชีพแล้ว ก็สามารถเรียกได้ว่าการหลอกลวงประสบความสำเร็จ โดยหลังจากมีการหลอกลวงแล้วนั้น ผู้เสียหายจะมีการแจ้งความร้องทุกข์ที่หน่วยงานที่เกี่ยวข้องต่อไป

๒. ผลกระทบของการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ต่อสังคมและผู้บริโภค

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สร้างผลกระทบอย่างยิ่งต่อประเทศไทย โดยเฉพาะอย่างยิ่งส่งผลกระทบต่อผู้บริโภคหรือประชาชนทั่วไปทั้งในเรื่องของการสูญเสียทรัพย์สินและความเป็นอยู่ของประชาชน เมื่อมีผลกระทบทางลบต่อประชาชนแล้วนั้นก็ไปสู่ความเสียหายต่อสังคม ในท้ายที่สุด ก็จะส่งผลประทบต่อประเทศ ทั้งในส่วนของเศรษฐกิจและความมั่นคงอีกด้วย โดยผลกระทบจากปัญหาดังกล่าวสามารถสรุปได้ดังนี้

๒.๑ ผลกระทบต่อความอยู่ดีมีสุขของประชาชน

การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สร้างผลกระทบประการที่สำคัญคือการที่ประชาชนจำนวนมากถูกหลอกและเสียทรัพย์สินให้กับมิจฉาชีพ นอกจากนี้ ยังมีรายงานว่าผู้ที่ตกเป็นเป้าหมายของมิจฉาชีพ มีความเสียหายทางสุขภาพจิต ไม่ว่าจะเป็นผู้เสียหายที่ได้เสียทรัพย์สินให้แก่มิจฉาชีพหรือไม่ โดยผู้ที่ได้มีการสูญเสียทรัพย์สินไปให้กับมิจฉาชีพมักจะรู้สึกโทษตัวเองที่เสียรู้ให้กับมิจฉาชีพ นอกจากผู้ตกเป็นเหยื่อจะต้องเผชิญปัญหาด้านสุขภาพจิตแล้ว ผู้ที่ตกเป็นเป้าหมายหรือถูกคุกคามจากมิจฉาชีพแม้ยังไม่มีการเสียทรัพย์มักประสบปัญหาวิตกกังวล หวาดระแวง และอาจมีการลบหรือบล็อกสายโทรเข้าหรือข้อความที่สำคัญไป ทำให้ไม่ได้รับข้อความหรือสายโทรเข้าจากเพื่อน ญาติ หรือผู้ที่มีความจำเป็นต้องติดต่ออีกด้วย

๒.๒ ผลกระทบต่อผู้ประกอบการและหน่วยงานที่เกี่ยวข้อง

ผลกระทบประการแรกที่เกิดขึ้นคือ หน่วยงานที่เกี่ยวข้องเกิดภาพลักษณ์ที่ไม่ดีต่อประชาชน เนื่องจากมิจฉาชีพมักนำชื่อหน่วยงานต่าง ๆ ไปแอบอ้าง โดยเฉพาะหน่วยงานรัฐที่เป็นที่รู้จักและมีความน่าเชื่อถือ จึงทำให้หน่วยงานนั้นเสียภาพลักษณ์ที่ดีไป ทั้งจากการที่ถูกนำไปแอบอ้างและมีประชาชนบางส่วนหลงเชื่อ และทั้งเมื่อเกิดปัญหาขึ้น ประชาชนจำนวนมากก็จะคาดหวังให้หน่วยงานต่าง ๆ รับผิดชอบกับปัญหาโดยการเข้ามาแก้ไขปัญหาให้หมดไป ซึ่งด้วยข้อจำกัดต่าง ๆ ก็อาจทำให้มีอุปสรรคในการแก้ปัญหาได้ นอกจากเสียภาพลักษณ์แล้ว ยังเสียทรัพยากรสำหรับการเตรียมระบบป้องกันมิจฉาชีพ ซึ่งทำให้สูญเสียทั้งทรัพยากร งบประมาณ และเวลา

๒.๓ ผลกระทบต่อสังคม

จากปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ที่เพิ่มมากขึ้น ทำให้ประชาชนที่รับรู้ข่าวสารอยู่ในภาวะวิตกกังวล และเกิดเป็นความหวาดระแวงต่อกันได้ กล่าวได้ว่าทำให้เกิดภาวะการไม่ไว้วางใจกันในสังคม เช่น การตัดสายเรียกเข้าจากเพื่อนหรือผู้ที่มีความจำเป็นต้องติดต่อ ทำให้เกิดปัญหาในภาพรวมของสังคมที่ผู้คนต่างก็เข้าถึงหรือติดต่อกันได้ยากขึ้น หรือเมื่อได้รับสายจากเพื่อนที่ได้รับความเดือดร้อนและต้องการความช่วยเหลือ แต่ด้วยการรับข่าวสารเกี่ยวกับการหลอกลวงที่เกิดขึ้น ทำให้เกิดความไม่ไว้วางใจว่าเป็นมิจฉาชีพหรือไม่ ด้วยภาวะเช่นนี้จึงเป็นทั้งผลกระทบที่เกิดขึ้นต่อความอยู่ดีมีสุขของประชาชนและเป็นผลกระทบต่อสังคมอีกด้วย

๒.๔ ผลกระทบต่อประเทศ

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่สามารถกล่าวได้ว่ามีผลกระทบต่อเศรษฐกิจของประเทศ เนื่องจากผู้เสียหายจะมีการโอนเงินให้กับมิจฉาชีพ และมิจฉาชีพจะถ่ายเททรัพย์สินออกนอกประเทศในที่สุด เมื่อประชาชนจำนวนถูกหลอกและเสียทรัพย์สินไปแล้ว ก็จะขาดความสามารถในการใช้จ่ายเพื่อขับเคลื่อนเศรษฐกิจภาพรวมของประเทศอีกด้วย นอกจากนี้การที่ประชาชนได้รับผลกระทบต่อความอยู่ดีมีสุข ยังพิจารณาได้ว่ากระทบต่อความมั่นคงของประเทศตามที่ได้กำหนดในยุทธศาสตร์ชาติ ๒๐ ปีอีกด้วย ด้วยเหตุนี้ ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่จึงเป็นปัญหาเร่งด่วนที่ต้องได้รับการแก้ไขและจำเป็นต้องมีแนวทางเพื่อป้องกันปัญหาที่จะเกิดขึ้นต่อไป

๓. สรุปการดำเนินมาตรการในการแก้ปัญหาและป้องกันการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในปัจจุบัน

ปัจจุบันหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนได้มีมาตรการหรือแนวทางในการแก้ปัญหาและป้องกันการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่มากมาย โดยมุ่งเน้นทั้งในส่วนของผู้กระทำผิด ผู้เสียหาย และโอกาสหรือช่องทางของการกระทำผิด ซึ่งเป็นองค์ประกอบสำคัญ ๓ ส่วนของอาชญากรรมตามทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) การดำเนินการในแต่ละส่วนในปัจจุบันมีดังนี้

๓.๑ ผู้กระทำผิด

แนวทางในการแก้ไขปัญหาที่มุ่งเน้นในส่วนของผู้กระทำผิดจะเป็นการวางกรอบแนวทางให้สามารถจับกุมผู้กระทำความผิดได้ และยังเป็นการป้องปรามผู้ที่คิดจะกระทำผิดซึ่งเป็นการป้องกันปัญหาที่จะเกิดขึ้นได้ด้วย โดยแนวทางในการแก้ไขและป้องกันปัญหาในส่วนของผู้กระทำผิดจะเน้นการบังคับใช้กฎหมายเป็นหลัก โดยทั่วไปแล้ว การกระทำผิดฐานหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา เช่น มาตรา ๓๔๑ ที่กำหนดโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ แต่เนื่องด้วยลักษณะของการกระทำผิดของขบวนการมิจฉาชีพในปัจจุบันที่เปลี่ยนแปลงไปมาก ทั้งพฤติกรรมการหลอกลวงและการใช้เครื่องมือต่าง ๆ รวมทั้งซิมม้าและบัญชีม้า จึงได้มีการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อให้มีบทลงโทษครอบคลุมทุกกลุ่มของมิจฉาชีพ รวมถึงพฤติกรรมการสนับสนุนการกระทำผิด เช่นการซื้อขายบัญชีม้าและซิมม้าที่มีกำหนดไว้ในมาตรา ๙ ๑๐ และ ๑๑ การบังคับใช้กฎหมายดังกล่าวนับเป็นการดำเนินการเพื่อแก้ไขและป้องกันปัญหาการ

หลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ และปัญหาอาชญากรรมทางเทคโนโลยีอื่น ๆ อีกทั้งยังเป็นการป้องปรามไม่ให้มีการกระทำผิดและการสนับสนุนการกระทำผิดที่จะเกิดขึ้นในอนาคต นอกจากนี้กฎหมายฉบับดังกล่าวยังกำหนดหน้าที่ให้หน่วยงานที่รับผิดชอบให้ความร่วมมือในการแก้ไขและป้องกันปัญหาอีกด้วย

๓.๒ ผู้เสียหาย

แนวทางในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในส่วนของผู้เสียหายจะสามารถแบ่งออกได้เป็น ๒ กลุ่มคือ แนวทางในการป้องกันผู้เสียหายจากมิจฉาชีพโดยมุ่งเน้นไปที่การแจ้งเตือนประชาชนและสร้างความตระหนักรู้ และแนวทางช่วยเหลือผู้เสียหายเมื่อถูกหลอกลวงแล้ว ในการป้องกันประชาชนจากมิจฉาชีพนั้น จะเป็นการป้องกันโดยใช้สร้างระบบการแจ้งเตือนต่าง ๆ ให้แก่ประชาชน เพื่อให้ทราบว่ากำลังถูกคุกคามจากมิจฉาชีพ แนวทางในการป้องกันการเข้าถึงในกลุ่มนี้ เช่น การเตือนผู้ใช้บริการเมื่อมีเลขหมายที่โทรมาจากต่างประเทศผ่าน VoIP โดยการใส่ Prefix “+๖๙๗” และ “+๖๙๘” ซึ่งมิจฉาชีพมักใช้การโทรจากต่างประเทศหรือการ Roaming จากต่างประเทศเข้ามา จึงเป็นการเตือนให้ผู้ใช้ระมัดระวังสายเรียกเข้าที่มี Prefix ดังกล่าว การให้มี Sender name ของผู้ส่งข้อความสั้น (SMS) โดยเฉพาะชื่อขององค์กรหรือบริษัทที่มักถูกมิจฉาชีพนำไปแอบอ้าง การพัฒนาแอปพลิเคชัน “กันกวน” ของสำนักงาน กสทช. ที่จะแจ้งเตือนผู้ใช้บริการเมื่อมีเลขหมายที่คาดว่าเป็นมิจฉาชีพติดต่อเข้ามา รวมทั้งยังมีการจัดทำฐานข้อมูลที่เป็นแหล่งความรู้ให้แก่ประชาชน เช่น การจัดทำฐานข้อมูลชื่อ “SCAM Alert/เท่าทันมิจฉาชีพ” ของสำนักงาน กสทช. การจัดตั้งศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.) ของ ธปท. นอกจากการแจ้งเตือนเมื่อมีสายเรียกเข้าหรือมีข้อความสั้นจากมิจฉาชีพแล้ว หากเป้าหมายถูกหลอกลวงได้สำเร็จและเข้าสู่ขั้นตอนของการโอนเงิน ธปท. ก็ได้มีการแจ้งเตือนบน mobile banking ก่อนทำธุรกรรมทุกครั้งอีกด้วย

หากมิจฉาชีพยังสามารถเข้าถึงเป้าหมายได้และหลอกลวงได้สำเร็จ หน่วยงานต่าง ๆ ก็มีแนวทางในการช่วยเหลือผู้เสียหาย เช่น การอำนวยความสะดวกให้ผู้เสียหายสามารถแจ้งความร้องทุกข์ได้อย่างสะดวกและรวดเร็ว ผู้เสียหายสามารถแจ้งความในพื้นที่ใดก็ได้ และสำนักงานตำรวจแห่งชาติยังจัดให้มีการแจ้งความออนไลน์ได้ที่ thaipoliceonline.com โดยพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้กำหนดขั้นตอนการดำเนินการที่เกี่ยวข้องการระงับธุรกรรมทางการเงินต้องสงสัยหลังจากมีการแจ้งความร้องทุกข์ไว้อย่างชัดเจน นอกจากนี้ยังมีการดำเนินการของ ธปท. ซึ่งได้กำหนดให้ทุกธนาคารมีช่องทางติดต่อเร่งด่วน (hotline) ตลอด ๒๔ ชั่วโมง และศูนย์คุ้มครองผู้ใช้บริการทางการเงินของตนเอง (Call center ๑๒๑๓) และยังมีการดำเนินการของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งได้จัดตั้งศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์ (ศูนย์ ๑๒๑๒ ETDA) เป็นต้น

๓.๓ โอกาสและช่องทางของการกระทำผิด

แนวทางในการแก้ไขและป้องกันปัญหาในส่วนของโอกาสและช่องทางของการกระทำผิดจะมุ่งเน้นไปที่การป้องกันเป้าหมายหรือประชาชนจากมิจฉาชีพโดยตัดโอกาสในการเข้าถึงประชาชนตั้งแต่ต้น จากการศึกษาวรรณกรรมที่เกี่ยวข้อง พบว่าการหลอกลวงของมิจฉาชีพได้โจมตีจุดอ่อนของมนุษย์ด้วยเทคนิคทางจิตวิทยา ทำให้เป้าหมายหลงกลได้ง่ายแม้ว่าจะเป็นผู้มีความรู้

ความสามารถมากก็ตาม ดังนั้น การปิดโอกาสในการเข้าถึงเป้าหมายตั้งแต่ต้นโดยไม่ต้องใช้วิจารณญาณของเป้าหมายในการเลือกที่จะรับสายมิจฉาชีพจึงเป็นทางเลือกที่ดีในการแก้ไขและป้องกันปัญหาการหลอกลวง ปัจจุบันหน่วยงานต่าง ๆ ได้เริ่มมีแนวทางในการปิดโอกาสหรือช่องทางการกระทำผิด เช่น สำนักงาน กสทช. ได้มีจัดทำบริการ USSD (Unstructured Supplementary Services Data) หมายเลข *๑๓๘ เพื่อให้ผู้ใช้บริการสามารถเลือกปฏิเสธการรับสายที่เป็นทราฟฟิกจากต่างประเทศได้ เป็นต้น

นอกจากการปิดกั้นโอกาสในการเข้าถึงเป้าหมายแล้ว ยังมีการปิดกั้นโอกาสในการโยกย้ายทรัพย์สินไปยังมือมิจฉาชีพด้วย โดย ธปท. ได้กำหนดให้มีการป้องกันมิให้มีช่องว่างในการใช้งานบัญชีและ Mobile banking ที่ทำให้มิจฉาชีพนำไปใช้ในการหลอกลวงได้ เช่น การจำกัดให้ผู้ใช้งาน ๑ บัญชีสามารถใช้ Mobile banking (username) ของแต่ละธนาคารได้ใน ๑ อุปกรณ์เท่านั้น การกำหนดให้ธนาคารต้องให้ผู้ใช้บริการยืนยันตัวตนขั้นต่ำด้วย biometrics เมื่อเปิดบัญชีแบบ Non-face-to-face หรือเมื่อเปลี่ยนวงเงิน หรือเมื่อมีการโอนเงินจำนวนมาก การกำหนดเพดานวงเงินถอนหรือโอนสูงสุดต่อวันบน Mobile banking ให้เหมาะสมตามระดับความเสี่ยงของกลุ่มผู้ใช้บริการแต่ละประเภท เป็นต้น

๓.๔ ภาพรวมของมาตรการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

การแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่นั้น นอกจากการกำหนดแนวทางในแต่ละองค์ประกอบของการกระทำผิด ก็ได้มีแนวทางที่กำหนดขึ้นเพื่อแก้ปัญหาในภาพรวมแบบบูรณาการระหว่างหน่วยงานต่าง ๆ ไว้ในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ โดยหน่วยงานที่เกี่ยวข้องได้แก่ สำนักงานตำรวจแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงาน กสทช. ผู้ให้บริการในกิจการโทรคมนาคม ธปท. และสถาบันการเงินต่าง ๆ เพื่อให้การดำเนินงานเป็นไปด้วยความราบรื่น พระราชกำหนดดังกล่าวยังได้กำหนดให้แต่งตั้งคณะกรรมการเพื่อกำหนดแนวทางในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และให้ข้อเสนอแนะเกี่ยวกับเหตุอันควรสงสัยตามพระราชกำหนดนี้ รวมทั้งให้คำแนะนำและคำปรึกษาเกี่ยวกับการปฏิบัติงานของเจ้าหน้าที่รัฐและหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามพระราชกำหนดนี้

อย่างไรก็ดี แม้ว่าปัจจุบันจะมีแนวทางในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่หลายประการซึ่งล้วนช่วยบรรเทาให้ความรุนแรงและความเสียหายของปัญหาดังกล่าวลดน้อยลง แต่จากการศึกษาวิเคราะห์ช่องว่างของแนวทางหรือมาตรการในการแก้ปัญหากับจุดประสงค์หรือเป้าหมายที่ไว้ พบว่ายังคงมีช่องว่างที่สามารถมีการปรับปรุงให้ดียิ่งขึ้นได้ งานศึกษาชิ้นนี้จึงเสนอแนวทางในการปิดช่องว่างดังกล่าวเหล่านั้น โดยได้เสนอเป็นข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหา ซึ่งการนำเสนอข้อเสนอแนะเป็นวัตถุประสงค์การวิจัยอีกข้อหนึ่ง และจะได้นำเสนอในลำดับถัดไป

ข้อเสนอแนะ

จากการวิเคราะห์ช่องว่าง (Gap Analysis) ระหว่างแนวทางหรือมาตรการในปัจจุบันกับรูปแบบพฤติกรรมการหลอกลวงและเป้าหมายที่ตั้งไว้ พบว่ายังมีช่องว่างที่จะสามารถต่อยอด เพื่อให้สามารถแก้ไขและป้องกันปัญหาการหลอกลวงได้อย่างมีประสิทธิภาพมากขึ้น โดยข้อเสนอแนะเชิงนโยบายและมาตรการประกอบด้วยข้อเสนอแนะ ๒ กลุ่ม คือข้อเสนอแนะเชิงนโยบายและข้อเสนอแนะเชิงปฏิบัติการ โดยข้อเสนอแนะทั้งสองกลุ่มเป็นข้อเสนอแนะที่มุ่งเน้นไปในเรื่องการป้องกันและป้องปรามก่อนที่ปัญหาจะเกิดขึ้น และการแก้ไขเมื่อปัญหาเกิดขึ้นแล้ว หรือทั้งสองส่วนประกอบกัน

ในภาพรวมของข้อเสนอแนะในการแก้ไขและป้องกันปัญหาการหลอกลวงนั้น จะเป็นการปรับปรุงและต่อยอดจากการดำเนินการที่มีอยู่แล้วเป็นหลัก ให้การดำเนินการที่มีอยู่แล้วนั้นมีประสิทธิภาพมากยิ่งขึ้น เช่น การบังคับใช้กฎหมายให้มีความแข็งขันมากยิ่งขึ้น หรือการนำกฎหมายที่มีอยู่แล้วมาใช้ให้เกิดประโยชน์สูงสุด รวมทั้งการปรับแก้กฎหมายให้มีบทลงโทษที่เหมาะสมครอบคลุมในทุกลักษณะของการกระทำผิด การสร้างความตระหนักรู้และให้ข้อมูลที่ครบถ้วนเพียงพอแก่ประชาชน ซึ่งหน่วยงานต่าง ๆ ได้มีการจัดตั้งศูนย์ข้อมูล แต่การประชาสัมพันธ์อาจยังไม่ครอบคลุมถึงประชาชนทุกกลุ่ม โดยเฉพาะอย่างยิ่งกลุ่มผู้ที่ยังขาดโอกาสในการเข้าถึงอินเทอร์เน็ต จึงมีข้อเสนอให้เพิ่มการประชาสัมพันธ์บนสื่อหลากหลายรูปแบบมากขึ้นทั้งรูปแบบออนไลน์ (Online) และออฟไลน์ (Offline) ปรับปรุงระบบการปิดกั้นสายเรียกเข้าจากมิจฉาชีพโดยนำระบบการยืนยันตัวตน เป็นต้น

นอกจากการปรับปรุงหรือเพิ่มเติมจากแนวทางหรือมาตรการที่มีอยู่แล้ว จากการศึกษาทั้งในกรณีที่เกิดขึ้นในประเทศไทยและต่างประเทศ พบว่าแนวทางที่ยังไม่มีการดำเนินการที่ชัดเจน จึงมีข้อเสนอแนะให้มีการริเริ่มและจัดทำแนวทางหรือมาตรการใหม่ขึ้น เพื่อสนับสนุนการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในปัจจุบันให้ดำเนินไปอย่างมีประสิทธิภาพและรอบด้านมากยิ่งขึ้น แนวทางหรือมาตรการใหม่ที่นำเสนอในงานศึกษานี้มาตรการแรกคือการสนับสนุนให้มีการเยียวยาและฟื้นฟูสุขภาพจิตของผู้เสียหายและผู้ที่ได้รับผลกระทบจากปัญหา เนื่องจากการศึกษาพบว่าปัญหาการหลอกลวงไม่เพียงแต่สร้างความเสียหายในแง่ของการเสียทรัพย์สิน แต่ยังมีความเสียหายทางจิตใจเกิดขึ้นอีกด้วย จึงควรมีแนวทางหรือมาตรการในการเยียวยาโดยอาจพิจารณาจัดตั้งศูนย์เยียวยาและฟื้นฟูสุขภาพจิตขึ้น หรืออาจสร้างความร่วมมือกับหน่วยงานต่าง ๆ ที่มีหน้าที่ในการดูแลสุขภาพจิตของประชาชนซึ่งเป็นผู้เชี่ยวชาญเฉพาะทาง เช่น กรมสุขภาพจิต กระทรวงสาธารณสุข การเยียวยาและฟื้นฟูสุขภาพจิตของผู้เสียหายและผู้ที่ได้รับผลกระทบนั้นนอกจากจะเป็นผลดีต่อความอยู่ดีมีสุขของประชาชนแล้ว ยังทำให้ผู้เสียหายมีกำลังใจที่ดีและยอมเปิดเผยข้อมูลที่จำเป็นต่อเจ้าหน้าที่ที่เกี่ยวข้องซึ่งเป็นประโยชน์อย่างยิ่งในการสืบสวนสอบสวนและแก้ไขปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย

นอกจากการเพิ่มเติมแนวทางหรือมาตรการในเรื่องการเยียวยาสุขภาพจิตแล้ว ในอีกด้านหนึ่งยังควรมีการสร้างความร่วมมือกันระหว่างหน่วยงานต่าง ๆ เพื่อการแก้ปัญหาแบบบูรณาการ โดยความร่วมมือดังกล่าวควรมีทั้งการการร่วมมือระหว่างหน่วยงานในประเทศ และความร่วมมือระหว่างประเทศ ทั้งในเรื่องของการนำเสนอและวางแนวทางหรือมาตรการต่าง ๆ ร่วมกัน การศึกษาปัญหาใน

เชิงลึก และการให้ความร่วมมือในการกระบวนการจับกุมผู้กระทำผิด เนื่องจากปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นปัญหาที่เกี่ยวพันกับหลายหน่วยงาน และต้องอาศัยความชำนาญของหลายภาคส่วน อีกทั้งปัญหาดังกล่าวมีลักษณะเหมือนอาชญากรรมข้ามชาติ ซึ่งต้องอาศัยความร่วมมือระหว่างประเทศในการแก้ไขปัญหาอีกด้วย

สิ่งสำคัญประการหนึ่งในการกำหนดแนวทางหรือมาตรการคือการคำนึงว่าการแก้ไขและป้องกันปัญหานั้นจะต้องเป็นการแก้ไขที่มุ่งเน้นไปที่การปกป้องประชาชนจากมิจฉาชีพทั้งการให้ประชาชนสามารถปกป้องตนเองได้ โดยให้มีความรู้เท่าทันต่อการหลอกลวง มีความตระหนักรู้ต่อปัญหา และสามารถรับมือได้อย่างถูกต้องเมื่อถูกคุกคามจากมิจฉาชีพรวมทั้งรับมือได้เมื่อถูกหลอกลวงแล้วด้วย ในขณะเดียวกัน หน่วยงานต่าง ๆ ก็จำเป็นต้องมีมาตรการหรือแนวทางป้องกันประชาชนตั้งแต่ต้น มิให้มิจฉาชีพเข้าถึงประชาชนได้ผ่านเทคโนโลยีการปิดกั้นโอกาสในการเข้าถึงต่าง ๆ ซึ่งแนวทางหรือมาตรการทั้งสองรูปแบบจำเป็นต้องดำเนินการร่วมกัน เพื่อปิดช่องว่างของโอกาสที่มิจฉาชีพจะสามารถเข้าถึงประชาชนได้มากที่สุด ในงานศึกษาฉบับนี้จึงได้นำเสนอมาตรการหรือแนวทางครบถ้วนทั้งสองส่วน เพื่อให้ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยบรรเทาทุเลาลง ซึ่งจะก่อให้เกิดความอยู่ดีมีสุขของประชาชน ขจัดสภาวะการไม่ไว้เนื้อเชื่อใจในสังคม เสริมสร้างความมั่นคงของประเทศและเศรษฐกิจในภาพรวมต่อไป

๑. ข้อเสนอแนะเชิงนโยบาย

ข้อเสนอแนะเชิงนโยบายโดยหลักจะมุ่งเน้นไปที่การปรับแก้กฎหมายที่มีอยู่ให้มีความเหมาะสมกับสถานการณ์และรูปแบบการหลอกลวงที่เปลี่ยนแปลงไปจากเดิม รวมทั้งเป็นการเสนอให้มีการใช้กฎหมายที่มีอยู่เพื่อให้เกิดประโยชน์สูงสุด โดยเฉพาะกฎหมายที่บังคับใช้เพื่อแก้ปัญหาแก๊งคอลเซ็นเตอร์ เช่น พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ข้อเสนอแนะเชิงนโยบายที่นำเสนอในส่วนนี้สามารถพิจารณาได้ว่าเป็นทั้งมาตรการเพื่อการป้องกันปัญหาที่จะเกิดขึ้นและเพื่อการป้องปรามผู้ที่คิดจะกระทำผิดด้วย นอกจากนี้ ยังเป็นมาตรการที่ใช้ในการแก้ไขปัญหา โดยจะเป็นส่วนสำคัญในกระบวนการจับกุมและดำเนินคดีผู้กระทำผิด ในขณะเดียวกัน ข้อเสนอแนะเชิงนโยบายยังสามารถพิจารณาได้ว่าเป็นข้อเสนอแนะที่มุ่งเน้นในส่วนของผู้กระทำผิด ซึ่งเป็นหนึ่งในสามองค์ประกอบตามทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) อีกด้วย ข้อเสนอแนะเชิงนโยบายมีดังนี้

๑.๑ การปรับแก้กฎหมายให้มีบทลงโทษที่เหมาะสม

บทลงโทษผู้กระทำผิดในปัจจุบันโดยหลักคือความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา โดยพบว่าบทลงโทษค่อนข้างน้อยเมื่อเทียบกับความผิดและความเสียหาย อีกทั้งยังมีบทลงโทษที่น้อยกว่ากลุ่มผู้ซื้อขายบัญชีและซิมม้า ผู้กระทำผิดที่โทรมาหลอกลวงมีความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา เช่น มาตรา ๓๔๑ ที่กำหนดโทษจำคุกไม่เกิน ๓ ปีหรือปรับไม่เกิน ๖ หมื่นบาท หรือทั้งจำทั้งปรับ ในขณะที่ผู้สนับสนุนการกระทำผิด เช่น การซื้อขายบัญชีม้าและซิมม้า ก็มีบทลงโทษเช่นกันตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีบทลงโทษในมาตรา ๙ ห้ามให้ผู้อื่นใช้บัญชีตนหรือบัญชีม้า และห้ามผู้อื่นใช้ซิมที่ลงทะเบียนในชื่อของตนหรือซิมม้า มีโทษจำคุกไม่เกิน ๓ แสนบาทหรือทั้งจำทั้งปรับ และหากเป็นกรณีที่เป็นคนจัดหาซื้อขายบัญชีม้าและซิมม้า มาตรา ๑๐ และ ๑๑ จะมีโทษจำคุก ๒-๕ ปี ปรับตั้งแต่ ๒ แสนถึง ๕ แสน

บาทหรือทั้งจำทั้งปรับ ซึ่งโทษจะไม่เท่ากับความผิดฐานฉ้อโกง จึงควรมีการกำหนดอัตราโทษของผู้กระทำผิดที่สูงขึ้น หรือให้มีความสอดคล้องกับการลงโทษกลุ่มสนับสนุนมิจฉาชีพที่กำหนดไว้ในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี อย่างไรก็ดี ความผิดฐานฉ้อโกงมีความครอบคลุมลักษณะอาชญากรรมที่หลากหลาย จึงอาจพิจารณาปรับปรุงบทลงโทษการกระทำความผิดโดยหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ หรือความผิดของอาชญากรรมทางเทคโนโลยี โดยให้มีการกำหนดลักษณะรายละเอียดและมีบทลงโทษเป็นการเฉพาะ

๑.๒ การบังคับใช้กฎหมายที่มีอยู่เพื่อให้เกิดประโยชน์สูงสุด

ควรสนับสนุนให้มีการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอย่างจริงจัง ทั้งในเรื่องกระบวนการจับกุม การประสานงานเพื่อให้ข้อมูลแก่เจ้าหน้าที่ตำรวจในกระบวนการสืบสวนสอบสวน และการลงโทษผู้กระทำผิดให้ครอบคลุมทั้ง ๓ กลุ่ม ผู้กระทำผิดหลัก ผู้สนับสนุน และนายทุน นอกจากนี้ เนื่องจากพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ได้มีการกำหนดให้หน่วยงานที่เกี่ยวข้องต้องมีการเปิดเผยหรือแลกเปลี่ยนข้อมูลแก่เจ้าหน้าที่ตำรวจเพื่อการสืบสวนสอบสวนแล้ว แนวทางที่ต้องมีการดำเนินการเพิ่มเติมคือการตกลงร่วมกันระหว่างหน่วยงานที่เกี่ยวข้องเพื่อกำหนดแนวทางของการเปิดเผยหรือแลกเปลี่ยนข้อมูล โดยควรมีระบบหรือกระบวนการที่เจ้าหน้าที่ที่เกี่ยวข้องสามารถได้รับข้อมูลไปใช้ในการสืบสวนสอบสวนอย่างทันท่วงที และผู้ให้ข้อมูลก็สามารถดำเนินการได้ รวมทั้งมีขั้นตอนการดำเนินการที่รัดกุมเพื่อมิให้ข้อมูลส่วนตัวของประชาชนรั่วไหลได้

๒. ข้อเสนอแนะเชิงปฏิบัติการ

นอกจากการข้อเสนอแนะที่เป็นแนวทางการแก้ไขและป้องกันปัญหาในเชิงนโยบายแล้ว มาตรการเชิงปฏิบัติการก็เป็นส่วนที่สำคัญในการดำเนินการแก้ไขและป้องกันปัญหา ในส่วนนี้ จะเป็นข้อเสนอแนะที่ครอบคลุมทั้งการแก้ไขปัญหาเมื่อปัญหานั้นได้เกิดขึ้นแล้ว ซึ่งมาตรการจะมุ่งเน้นไปที่ผู้เสียหายและผู้กระทำผิด เช่น การเยียวยาความเสียหาย การดำเนินการจับกุมและลงโทษผู้กระทำผิดที่สอดคล้องกับกฎหมายที่มีอยู่ ดังที่ได้มีการอธิบายในข้อเสนอแนะเชิงนโยบาย และครอบคลุมทั้งการป้องกันและป้องปรามซึ่งเป็นการลดโอกาสที่ปัญหาจะเกิดขึ้น ข้อเสนอแนะส่วนนี้มักมุ่งเน้นไปที่โอกาสหรือช่องทางในการกระทำผิด และการป้องกันปัญหาในองค์รวม เช่น การสร้างความตระหนักรู้แก่ประชาชน ปิดกั้นโอกาสที่มิจฉาชีพจะสามารถเข้าถึงประชาชนได้ และการจัดตั้งกรอบความร่วมมือของหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ ข้อเสนอแนะเชิงปฏิบัติการจะการนำเสนอตาม ๓ องค์ประกอบของทฤษฎีสามเหลี่ยมอาชญากรรม เริ่มจากข้อเสนอแนะที่มุ่งเน้นไปที่ผู้เสียหายหรือประชาชนทั่วไป ซึ่งเป็นส่วนที่มีความสำคัญมากที่สุด จากนั้นจึงนำเสนอข้อเสนอแนะที่มุ่งเน้นไปที่ผู้กระทำผิด โอกาสหรือช่องทางการกระทำผิด และสุดท้ายคือมาตรการการแก้ปัญหาในภาพรวม โดยข้อเสนอแนะเชิงปฏิบัติการของงานวิจัยนี้มีดังนี้

๒.๑ ข้อเสนอแนะในการแก้ไขและป้องกันปัญหาในส่วนของผู้เสียหาย/ประชาชน

๒.๑.๑ แนวทางในการป้องกันประชาชนจากมิจฉาชีพ

- การสร้างความตระหนักรู้และให้ข้อมูลแก่ประชาชนอย่างครอบคลุมทุกกลุ่ม

การแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ที่สำคัญประการหนึ่งคือการสร้างความตระหนักรู้และให้ความรู้แก่ประชาชน เพื่อมิให้ตกเป็นผู้เสียหายได้ อย่างไรก็ดี พบว่าการประชาสัมพันธ์หรือให้ข้อมูลแก่ประชาชนผ่านสื่อต่าง ๆ อาจยังไม่เพียงพอ ด้วยประชาชนบางกลุ่มยังขาดโอกาสในการเข้าถึงสื่อ จึงควรมีการใช้สื่อประชาสัมพันธ์ที่หลากหลายมากขึ้นทั้งสื่อออนไลน์ (Online) และสื่อออฟไลน์ (Offline) โดยคำนึงถึงข้อจำกัดในการเข้าถึงสื่อของประชาชนทุกกลุ่ม รวมทั้งผู้ด้อยโอกาสต่าง ๆ เพื่อให้ข้อมูลถูกส่งต่อไปยังประชาชนให้มากที่สุด โดยประชาชนควรต้องมีความรู้ความเข้าใจต่อปัญหา ลักษณะการหลอกลวง การรับมือกับมิจฉาชีพเมื่อถูกคุกคาม เพื่อให้สามารถปกป้องตนเองได้ นอกจากนี้ ประชาชนควรต้องมีความรู้ความเข้าใจว่าหากตนเองตกเป็นผู้เสียหายแล้ว จะต้องดำเนินการอย่างไร หรือติดต่อช่องทางใดเพื่อได้รับความช่วยเหลือที่ถูกต้องโดยเร็วที่สุด

๒.๑.๒ แนวทางในการแก้ไขและเยียวยาผู้เสียหาย

๑) การเยียวยาสุขภาพจิตของผู้เสียหาย

ควรมีการพิจารณาประเด็นเรื่องปัญหาสุขภาพจิตของผู้เสียหายจากการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ เพื่อให้มีการจัดตั้งศูนย์เยียวยาและฟื้นฟูสุขภาพจิตของผู้เสียหายและผู้ที่เกี่ยวข้องกับผู้เสียหาย ซึ่งแนวทางนี้เป็นแนวทางที่มีการนำมาใช้เป็นอย่างแพร่หลายในต่างประเทศ นอกจากนี้ ศูนย์ฟื้นฟูและเยียวยาสุขภาพจิตยังสามารถทำหน้าที่สนับสนุนผู้เสียหายให้มีกำลังใจในการให้ข้อมูลที่จำเป็นต่อเจ้าหน้าที่ที่เกี่ยวข้อง เพราะข้อมูลดังกล่าวเป็นประโยชน์ต่อกระบวนการจับกุมและกำหนดมาตรการที่เหมาะสม ศูนย์เยียวยาและฟื้นฟูสุขภาพจิตควรต้องมีเจ้าหน้าที่ที่มีความชำนาญเฉพาะทาง โดยประเด็นนี้ควรเชิญหน่วยงานที่มีความเชี่ยวชาญในเรื่องสุขภาพจิตเข้ามามีส่วนร่วม เช่น กรมสุขภาพจิต กระทรวงสาธารณสุข

๒) การจัดทำช่องทางการร้องเรียนที่เป็นศูนย์กลางของการร้องเรียน

ในการช่วยเหลือผู้เสียหายนั้น ควรต้องมีช่องทางในการติดต่อหน่วยงานที่เกี่ยวข้องที่รวดเร็วเพื่อให้มีความช่วยเหลือที่ทันท่วงทีได้ โดยในปัจจุบันได้มีช่องทางมากมายจากหลายหน่วยงาน แต่พบว่าแต่ละหน่วยงานต่างก็มีช่องทางการติดต่อของตัวเอง จึงอาจพิจารณาการใช้เลขหมายเดียวกันหรือมีช่องทางในลักษณะของศูนย์กลางในการติดต่อเฉพาะเรื่องปัญหาอาชญากรรมทางเทคโนโลยี เพื่อไม่ให้ประชาชนเกิดความสับสน

๒.๒ ข้อเสนอแนะในการแก้ไขและป้องกันปัญหาในส่วนของผู้กระทำผิด

- การจัดตั้งความร่วมมือระหว่างประเทศ

การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นปัญหาที่มีลักษณะคล้ายคลึงกับอาชญากรรมข้ามชาติ การจับกุมและการแก้ไขปัญหาจึงต้องอาศัยความร่วมมือระหว่าง

ประเทศ ดังนั้น จึงต้องมีความร่วมมือระหว่างประเทศอย่างเป็นทางการในรูปแบบต่าง ๆ ทั้งการสร้างความร่วมมือใหม่ เช่น การทำ Memorandum of Understandings (MoU) หรือสนธิสัญญา (Treaty) ในระดับทวิภาคี และพัฒนาจากความร่วมมือเดิมที่มีอยู่ เช่น กรอบความร่วมมือ Association of Southeast Asian Nations (ASEAN) โดยความร่วมมือระหว่างประเทศอาจเป็นทั้งความร่วมมือในการจับกุม การวางแนวทางในการป้องกันปัญหา รวมทั้งการนำเสนอวิธีการหรือเทคโนโลยีใหม่ ๆ ที่เป็นประโยชน์ต่อประเทศสมาชิก

๒.๓ ข้อเสนอแนะในการปิดกั้นโอกาสและช่องทางในการกระทำผิด

- การปรับปรุงระบบการแจ้งเตือนประชาชนเมื่อมีการติดต่อจากมิจฉาชีพโดยนำเทคโนโลยีต่าง ๆ มาใช้

นอกจากการสร้างความตระหนักรู้แล้ว ควรมีมาตรการป้องกันหรือปกป้องประชาชนจากการเข้าถึงของมิจฉาชีพ โดยการนำเทคโนโลยีต่าง ๆ มาใช้ เพื่อลดโอกาสที่ประชาชนจะถูกหลอกได้ โดยการป้องกันประการแรกคือการแจ้งเตือนให้ประชาชนทราบเมื่อมีการติดต่อจากมิจฉาชีพ เช่น ควรมีการพิจารณานำระบบ Sender name มาใช้ในการโทรด้วย และอาจมีการพิจารณานำระบบตรวจสอบตัวตนของผู้โทรมาใช้ ดังที่มีตัวอย่างการใช้ในต่างประเทศ เช่น ระบบ CLI ของสหราชอาณาจักร หรือระบบ STIR/SHAKEN ของสหรัฐอเมริกา โดยนอกจากการใช้ระบบดังกล่าวจะสามารถช่วยตรวจสอบตัวตนของผู้โทรแล้ว ยังสามารถช่วยกรองเลขหมายที่เป็นเลขหมายของมิจฉาชีพโดยผู้ใช้บริการไม่จำเป็นต้องมีการติดต่อพูดคุยกับมิจฉาชีพ ซึ่งเป็นการปิดโอกาสของมิจฉาชีพที่จะหลอกลวงประชาชนได้

๒.๔ ข้อเสนอแนะสำหรับแนวทางในการแก้ปัญหาในภาพรวม

- การจัดตั้งความร่วมมือแบบบูรณาการของหน่วยงานที่เกี่ยวข้องทั้งหมด

อาจมีการจัดตั้งความร่วมมืออื่น ๆ เพิ่มเสริมการจัดตั้งคณะกรรมการของพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ โดยต้องมีลักษณะเป็นการบูรณาการของภาคส่วนต่าง ๆ ทั้งภาครัฐและเอกชน โดยอาจใช้ตัวอย่างการดำเนินการที่ผ่านมาเป็นแนวทางเบื้องต้น เช่น การจัดตั้งคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก๊งโทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง ความร่วมมือนี้ควรเป็นการร่วมมือของหน่วยงานที่เกี่ยวข้องและได้รับผลกระทบ และหน่วยงานที่มีความเชี่ยวชาญเฉพาะทาง เพื่อให้มีการแก้ไขปัญหา นำเสนอมาตรการ และสามารถนำไปปฏิบัติให้เห็นผลได้

๓. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่เป็นปัญหาที่มีความรุนแรงและมีการเปลี่ยนแปลงอย่างรวดเร็ว กล่าวได้ว่าเป็นปัญหาที่มีพลวัตสูง ด้วยเหตุนี้ จึงเป็นปัญหาที่ควรมีการติดตามอย่างใกล้ชิด รวมถึงต้องมีการศึกษาเพิ่มเติมอยู่เสมอด้วยเช่นกัน เพื่อให้งานศึกษาที่เกี่ยวข้องในอนาคตได้สามารถเสนอแนวทางที่เหมาะสมมากยิ่งขึ้น จึงขอเสนอแนวทางสำหรับงานศึกษาในอนาคต ซึ่งเป็นการต่อยอดและเสริมจากงานศึกษานี้ที่ยังคงมีข้อจำกัดหลายประการ โดยข้อเสนอแนะดังกล่าวมีดังนี้

๓.๑ เนื่องจากงานศึกษานี้ยังมีข้อจำกัดในเรื่องของการเก็บข้อมูล โดยยังขาดข้อมูลที่มาจากมิจฉาชีพ ปัจจุบันยังมีจำนวนผู้กระทำผิดที่ถูกจับกุมได้ในจำนวนที่น้อย การเข้าถึงมิจฉาชีพ

และเก็บข้อมูลจึงยังคงกระทำได้ยาก ข้อมูลดังกล่าวเป็นประโยชน์อย่างยิ่งต่อการกำหนดแนวทางหรือมาตรการในการแก้ไขและป้องกันปัญหา โดยเฉพาะข้อมูลทั้งในส่วนของพฤติกรรมการหลอกลวง รูปแบบของขบวนการหลอกลวง ที่มาของแหล่งทุน และแรงจูงใจของการกระทำผิด ซึ่งจะทำให้ผู้ศึกษาเข้าใจที่มาของการตัดสินใจกระทำผิด และเสนอแนะแนวทางในการแก้ไขปัญหาได้ดียิ่งขึ้น

๓.๒ นอกจากข้อมูลในส่วนของผู้กระทำผิดแล้ว ข้อมูลในส่วนของผู้เสียหายก็เป็นข้อมูลที่สำคัญยิ่งเช่นเดียวกัน โดยผู้เสียหายจะเป็นผู้ที่สามารถให้ข้อมูลที่สำคัญทั้งรายละเอียดการหลอกลวง สาเหตุหรือปัจจัยต่าง ๆ ที่ทำให้ผู้เสียหายหลงเชื่อมิจฉาชีพ ปัญหาที่ผู้เสียหายประสบหรือผลกระทบที่ได้รับทั้งในด้านเศรษฐกิจและสุขภาพจิต และสิ่งที่ผู้เสียหายต้องการได้รับความช่วยเหลือจากหน่วยงานต่าง ๆ จึงเสนอแนะแนวทางสำหรับงานในอนาคตว่าอาจมีการพิจารณาเก็บข้อมูลจากผู้เสียหาย และอาจรวมถึงบุคคลรอบข้างผู้เสียหายด้วย อย่างไรก็ดี การเข้าถึงผู้เสียหายเป็นกระบวนการที่มีความซับซ้อน และอาจกระทบต่อสิทธิส่วนบุคคลได้โดยง่าย จึงต้องใช้ความระมัดระวังในกระบวนการวิจัยเพื่อมิให้ผู้เสียหายได้รับผลกระทบเพิ่มเติม

๓.๓ งานศึกษานี้มีขอบเขตของการศึกษาที่มุ่งเน้นไปในเรื่องของผลกระทบของปัญหาการหลอกลวง แนวทางหรือมาตรการต่าง ๆ และมีขอบเขตของการศึกษาในเรื่องสังคมจิตวิทยา จึงอาจยังมีการพิจารณาและวิเคราะห์ในประเด็นอื่น ๆ ในระดับเบื้องต้นเท่านั้น โดยประเด็นเหล่านี้ยังสามารถมีการศึกษาเพิ่มเติมในเชิงลึกได้ เช่น ประเด็นทางเทคโนโลยี ความเหมาะสม ข้อดีข้อเสียของการนำระบบยืนยันตัวตนต่าง ๆ มาใช้ในกรณีของประเทศไทย เป็นต้น

๓.๔ เนื่องจากงานศึกษานี้มุ่งเน้นไปที่การหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่และข้อความสั้นเป็นหลัก จึงยังไม่มีการศึกษาในเชิงลึกในส่วนที่เป็นการหลอกลวงผ่านสื่อโซเชียลมีเดียและแอพพลิเคชั่นต่าง ๆ ซึ่งขั้นตอนการหลอกลวงรวมทั้งการได้มาซึ่งข้อมูลของเป้าหมายอาจมีความแตกต่างกันได้ งานศึกษาในอนาคตจึงอาจศึกษาเพิ่มเติมในรูปแบบการหลอกลวงผ่านโซเชียลมีเดียหรือสื่อออนไลน์อื่น ๆเพิ่มเติม เพื่อให้มีข้อมูลของการหลอกลวงครบถ้วนทุกรูปแบบ และหน่วยงานต่าง ๆ สามารถนำข้อมูลที่ครบถ้วนนี้ไปใช้ประโยชน์ได้มากขึ้น

บรรณานุกรม

ภาษาไทย

วารสาร

จักรพงษ์ กังวานโสภณ. “ความผิดฐานฉ้อโกง : ศึกษากรณีการหลอกลวงทางโทรศัพท์ (แก๊งคอลเซ็นเตอร์)”. วารสารสถาบันวิจัยและพัฒนา มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา. ๗ (๑), มกราคม – มิถุนายน ๒๕๖๕. หน้า ๒๘๐ - ๒๙๐.

วิทยานิพนธ์ รายงานการวิจัย

พัลลภ หริ่งรอด, พ.ต.ต. “มาตรการตามกฎหมายในการปราบปรามองค์กรอาชญากรรมข้ามชาติ ศึกษาเฉพาะกลุ่มคอลเซนเตอร์”. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขาวิชากฎหมายอาญาและอาชญาวิทยา, มหาวิทยาลัยบูรพา, ๒๕๖๒.

สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และนัทธี จิตสว่าง. “อาชญากรรมข้ามชาติ: ภัยคุกคามประเทศไทยเกี่ยวกับแก๊งคอลเซ็นเตอร์”. รายงานการวิจัย, จุฬาลงกรณ์มหาวิทยาลัย, ภาควิชาสังคมและมานุษยวิทยา, คณะรัฐศาสตร์, ๒๕๖๓.

ประกาศ

“ประกาศสำนักนายกรัฐมนตรี เรื่อง การประกาศแผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ. ๒๕๖๑ - ๒๕๘๐)”. ราชกิจจานุเบกษา. เล่มที่ ๑๓๖, ๑๘ เมษายน ๒๕๖๒, หน้า ๑ – ๓๙๖.

ภาษาต่างประเทศ

Books

Cialdini, Robert B. “Influence: Science and Practice”. Massachusetts: Allyn and Bacon, 2001.

Journals and Newspapers

Button, Mark and others. “Online frauds: Learning from victims why they fall for these scams”, Australian & New Zealand Journal of Criminology. 47 (3), 2014. p. 391-408.

Choi, Kyung-schick, Choo, Kyungseok and Sung, Yong-eun. “Demographic variables and risk factors in computer-crime: an empirical assessment”. Cluster Computing. 19, 2016. p.369-377.

Cialdini, Robert B. and Goldstein, Noah J. “The Science and Practice of Persuasion”, Cornell Hotel and Restaurant Administration Quarterly. 43 (2), 2002. p.40-50.

Coluccia, Anna and others. “Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review”. Clinical Practice & Epidemiology in Mental Health. 16, 2020. p. 24-35.

Kraiwanit, Tanpat and Srijaem, Piroonrat. “Evaluation of Internet Transaction Fraud in Thailand”. Indian Journal of Economics & Business. 20 (1), 2021. p. 195-204.

Stejano, Frank and Wilson, Paul. “Understanding Scam Victims: Seven Principles for Systems Security”, Communications of the ACM. 54 (3), 2011. p. 70-75

Whitty, Monica T. and Buchanan, Tom. “The Online Dating Romance Scam: A Serious Crime”, CyberPsychology, Behavior, and Social Networking. 15 (3), 2012. p. 181-183.

Whitty, Monica T. “The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam”, British Journal of Criminology. 53, 2013. p. 665-684.

Research, Report and Thesis

ACCC. “Targeting scams: Report of the ACCC on scams activity 2021”. Report, ACCC, 2022.

ACMA. “Combating scams: Action plan summary”. Report, ACMA, 2019.

FBI. “Internet Crime Report 2021”. Report, Internet Crime Complaint Center, Federal Bureau of Investigation, 2022.

ICO. “Operation LINDEN: Unsolicited Marketing Communications Strategy Meeting”. Meeting Report, ICO, 2020.

Lea, Stephen E.G., Fischer, Peter and Evans, Kath M. “The psychology of scams: Provoking and committing errors of judgement”. Consultancy Report, Office of Fair Trading, 2009.

Modic, David. “Willing to be scammed: How self-control impacts Internet scam compliance”. Doctoral thesis, University of Exeter, 2012.

Modic, David and Lea, Stephen E.G., “Scam Compliance and the Psychology of Persuasion”. Research Article, University of Exeter, 2013.

Ofcom. “Tackling scam calls and texts: Ofcom’s role and approach”. Report of Policy Positioning Statement, Ofcom, 2022.

Stejano, Frank and Wilson, Paul. “Understanding scam victims: seven principles for systems security”. Technical Report, University of Cambridge, 2009.

Tversky, Amos and Kahneman, Daniel. “Judgment under uncertainty: Heuristics and Biases”. Technical Report, Office of Naval Research Advanced Research Projects Agency, 1973.

Electronic Database

ACMA. “Avoid sending spam”. ACCC. June 9, 2022. (Online). Available: https://www.acma.gov.au/avoid-sending-spam

ACMA. “New rules to fight SMS scams”. ACMA. July 12, 2022. (Online). Available: https://www.acma.gov.au/articles/2022-07/new-rules-fight-sms-scams

Bhattacharjee, Yudhijit. “Who’s Making All Those Scam Calls?”, The New York Times Magazine. January 27, 2021. (Online). Available: https://www.nytimes.com/2021/01/27/magazine/scam-call-centers.html

CFPB. “Beware of scammers pretending to be from the CFPB”, Consumer Financial Protection Bureau. September 1, 2022. (Online). Available: https://www.consumerfinance.gov/about-us/blog/beware-of-scammers-pretending-to-be-from-the-cfpb/

Chua, Nadine and Sun, David. “Fake friend call scam reports spike by more than 200% in Singapore; victims lose $8.8m in 2022”. The Straits Times. February 9, 2023. (Online). Available: https://www.straitstimes.com/singapore/over-200-spike-in-fake-friend-call-scam-reports-in-2022-victims-lost-88-million

FCC. “Robocall Response Team: Combating Scam Robocalls & Robotexts”, Federal Communications Commission. August 18, 2022. (Online). Available: https://www.fcc.gov/spoofed-robocalls

FTC. “How to Recognize and Report Spam Text Messages”, Federal Trade Commission Consumer Advice. July 2022. (Online). Available: https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

FTC. “The Do Not Call Registry”, Federal Trade Commission. n.d. (Online). Available: https://www.ftc.gov/news-events/topics/do-not-call-registry

IMDA. “Anti-Scam Measures”. IMDA. January 23, 2023. (Online). Available: https://www.imda.gov.sg/How-We-Can-Help/Anti-Scam-Measures

Mobile UK. “SMS PhishGuard- Upping the ante in the fight against fraud”. Mobile UK. November 27, 2018. (Online). Available: https://www.mobileuk.org/news/sms-phishguard-upping-the-ante-in-the-fight-against-fraud

Preiskel & Co. “Ofcom publishes new rules for telecoms providers to combat scam calls”, Preiskel & Co. November 23, 2022. (Online). Available: https://www.preiskel.com/ofcom-publishes-new-rules-for-telecoms-providers-to-combat-scam-calls/

Scamwatch. “Scamwatch role”, ACCC. n.d. (Online). Available: https://www.scamwatch.gov.au/about-scamwatch/scamwatch-role

Tham, Davina. “S$661 million lost to scams in 2022, with young adults most likely to fall victims: SPF”. Channel News Asia. February 8, 2023. (Online). Available: https://www.channelnewsasia.com/singapore/police-scam-cybercrime-statistics-young-adults-2022-3262141

ประวัติย่อผู้วิจัย

ชื่อ นายไตรรัตน์ วิริยะศิริกุล

วัน เดือน ปีเกิด ๑๒ พฤษภาคม ๒๕๑๓

การศึกษา

ประถมศึกษา โรงเรียนอัสสัมชัญ พ.ศ. ๒๕๑๙ – ๒๕๒๔

มัธยมศึกษา โรงเรียนอัสสัมชัญ บางรัก พ.ศ. ๒๕๒๕ – ๒๕๓๐

ปริญญาตรี ศิลปศาสตร์บัณฑิต (เอกอังกฤษธุรกิจ)
มหาวิทยาลัยอัสสัมชัญ (ABAC) พ.ศ. ๒๕๓๕

ปริญญาโท MS. in Leadership and Management
University of La Verne , CA., USA. พ.ศ. ๒๕๓๗

ประวัติการทำงานโดยย่อ

พ.ศ. ๒๕๓๕ Sales Representative , Nestle Products (Thailand) Inc.

พ.ศ. ๒๕๓๗ Account Executive , Lintas (Thailand) Co., Ltd.

พ.ศ. ๒๕๓๘ Senior Sales Representative , Nestle Products (Thailand) Inc.

พ.ศ. ๒๕๓๘ - ๒๕๔๗ เจ้าหน้าที่วิเคราะห์งบประมาณ
สำนักงบประมาณ สำนักนายกรัฐมนตรี

ม.ค. ๒๕๔๘ – ก.ย. ๒๕๕๐ ผู้อำนวยการส่วนกิจการประธานกรรมการ
สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ

ก.ย. ๒๕๕๐ – ก.ย. ๒๕๕๑ ผู้อำนวยการสำนักประธานกรรมการสำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ

ก.ย. ๒๕๕๑ – พ.ค. ๒๕๕๕ ผู้อำนวยการสำนักกิจการกรรมการสำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ

พ.ค. ๒๕๕๕ - ม.ค. ๒๕๕๖ ผู้อำนวยการกลุ่มงานกรรมการกิจการโทรคมนาคม
รักษาการแทนรองเลขาธิการ กสทช. ภารกิจยุทธศาสตร์และกิจการองค์กร
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

ก.พ. ๒๕๕๖ – มิ.ย. ๒๕๖๓	รองเลขาธิการ กสทช. สายงานยุทธศาสตร์และกิจการองค์กร สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
ก.ค. ๒๕๖๓ – ปัจจุบัน	รองเลขาธิการ รักษาการแทน เลขาธิการ กสทช. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

ตำแหน่งปัจจุบัน รองเลขาธิการ รักษาการแทน เลขาธิการ กสทช.
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

สรุปย่อ

ลักษณะวิชา สังคมจิตวิทยา

เรื่อง นโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

ผู้วิจัย นายไตรรัตน์ วิริยะศิริกุล **หลักสูตร** วปอ. **รุ่นที่** 65

ตำแหน่ง รองเลขาธิการ รักษาการแทน เลขาธิการ กสทช.

ความเป็นมาและความสำคัญของปัญหา

ปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่โดยเฉพาะอย่างยิ่งภัยการหลอกลวงทางโทรศัพท์มิจฉาชีพคอลเซ็นเตอร์ หรือแก๊งคอลเซ็นเตอร์ (Call Center) ถือเป็นอาชญากรรมทางสังคมร้ายแรงในปัจจุบันซึ่งส่งผลกระทบกับประชาชนในวงกว้างและกระทบต่อความมั่นคงของประเทศอย่างมีนัยสำคัญ โดยจากข้อมูลในปี 2564 มีผู้เสียหายเข้าแจ้งความกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กว่า 1,600 ราย มูลค่าความเสียหายสูงกว่า 1,000 ล้านบาท และจากข้อมูลของ บช.สอท. ระหว่างวันที่ 1 มีนาคม – 10 ธันวาคม 2565 ซึ่งผู้เสียหายได้แจ้งความออนไลน์ มีผู้เสียหายจากการหลอกลวงทางโทรศัพท์ถึง 11,060 คดี คิดเป็นร้อยละ 7.65 และสูงเป็นอันดับที่ 5 ของจำนวนคดีอาชญากรรมทางเทคโนโลยีทั้งหมด โดยมีมูลค่าความเสียหายสูงถึง 2,320 ล้านบาท และยังมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องและรวดเร็ว นอกจากความเสียหายทางเศรษฐกิจแล้ว ยังพบว่าปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ยังส่งผลกระทบอย่างมากต่อความอยู่ดีมีสุขของประชาชน สังคม และต่อประเทศชาติรวมทั้งความมั่นคง ซึ่งเป็นเป้าหมายสำคัญในยุทธศาสตร์ชาติด้านความมั่นคงที่จะต้องบริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคงปลอดภัย ตามแนวคิด “ความมั่นคงแบบองค์รวม” อีกด้วย

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม (สำนักงาน กสทช.) ในฐานะหน่วยงานหลักในการกำกับดูแลกิจการโทรคมนาคมได้ตระหนักถึงภัยจากการหลอกลวงดังกล่าว และเห็นถึงความจำเป็นของการแก้ไขและป้องกันปัญหาอย่างมีประสิทธิภาพ งานวิจัยนี้จึงเป็นการศึกษาปัญหาดังกล่าวโดยละเอียดตั้งแต่พฤติกรรมในการหลอกลวงและผลกระทบที่เกิดขึ้นต่อสังคมและผู้บริโภค แนวทางการดำเนินการในการแก้ไขหรือป้องกันการหลอกลวง เพื่อนำเสนอข้อเสนอแนะทั้งข้อเสนอแนะเชิงนโยบายและเชิงปฏิบัติการ และมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ ทั้งในส่วนของหน่วยงานภาครัฐที่เกี่ยวข้อง ผู้ให้บริการโทรศัพท์เคลื่อนที่ ผู้ให้บริการโทรคมนาคมที่เกี่ยวข้อง และผู้บริโภค

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาพฤติกรรมในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ และผลกระทบที่เกิดขึ้นต่อสังคมและผู้บริโภค

2. เพื่อศึกษาแนวทางการดำเนินการในการแก้ไขหรือป้องกันการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในปัจจุบัน

3. เพื่อนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา การวิจัยนี้มุ่งเน้นการศึกษาเฉพาะพฤติกรรมที่เกิดขึ้นในการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในส่วนที่เกิดขึ้นกับกลุ่มบุคคลทั่วไปและแนวทางการดำเนินการของหน่วยงานที่เกี่ยวข้องทั้งในประเทศ และในต่างประเทศ

2. ขอบเขตด้านประชากร กลุ่มเป้าหมายที่จะดำเนินการเก็บข้อมูลผ่านการสัมภาษณ์เชิงลึก (In-depth Interview) มี 2 กลุ่ม ได้แก่ กลุ่มเจ้าหน้าที่ตำรวจ และกลุ่มผู้แทนในคณะทำงานพหุภาคีเพื่อแก้ไขปัญหาแก็งค์โทรศัพท์ (Call Center) และข้อความสั้น (SMS) หลอกลวง

วิธีดำเนินการวิจัย

ผู้วิจัยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยดำเนินการ ดังนี้

1. การรวบรวมข้อมูล งานวิจัยนี้ได้ใช้เครื่องมือในการรวบรวมข้อมูล 2 วิธี

1.1 การศึกษาเอกสาร (Documentary Research) ซึ่งผู้วิจัยจะดำเนินการศึกษาข้อมูลทุติยภูมิผ่านเอกสารที่เกี่ยวข้อง

1.2 การสัมภาษณ์เชิงลึก (In-depth Interview) ซึ่งเป็นการดำเนินการศึกษาข้อมูลปฐมภูมิกับบุคคลผู้ที่เกี่ยวข้อง ซึ่งมีประชากรหรือกลุ่มตัวอย่างรวม 6 ท่าน ได้แก่ ผู้แทนกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ผู้แทนธนาคารแห่งประเทศไทย ผู้แทนจากผู้ให้บริการโทรคมนาคม และผู้ช่วยเลขาธิการ กสทช. ด้านกิจการโทรคมนาคม

2. การวิเคราะห์ข้อมูล ในการวิเคราะห์ข้อมูลนั้น ผู้วิจัยใช้วิธีการวิเคราะห์ช่องว่าง (Gap Analysis) เพื่อหาความแตกต่างระหว่างรูปแบบและพฤติกรรมการหลอกลวงกับการดำเนินมาตรการในการแก้ไขและป้องกันปัญหาดังกล่าว งานวิจัยนี้ยังได้มีการวิเคราะห์โดยใช้ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ซึ่งเป็นทฤษฎีพื้นฐานในการอธิบายและวิเคราะห์องค์ประกอบต่าง ๆ ในการกระทำผิด และมีการใช้หลักการทางจิตวิทยาในการอธิบายพฤติกรรมและลักษณะของการหลอกลวงของมิจฉาชีพ รวมทั้งกระบวนการตัดสินใจของเป้าหมายเมื่อถูกมิจฉาชีพหลอกลวงอีกด้วย

3. การนำเสนอข้อมูล นำเสนอข้อมูลและสรุปผลการศึกษาซึ่งอธิบายเชื่อมโยงข้อค้นพบเพื่อนำไปสู่การนำเสนอข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทยแบบบูรณาการ

ผลการวิจัย

ลักษณะสำคัญของพฤติกรรมการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่

1. มิจฉาชีพมีการทำงานเป็นกลุ่มขบวนการ มิจฉาชีพมีการทำงานกันเป็นขบวนการและแบ่งหน้าที่กันทำอย่างชัดเจน หรือที่เรียกว่าเป็น “แก๊ง” โดยทั่วไปแล้ว จะประกอบด้วย 3 กลุ่มหลัก คือ (1) มิจฉาชีพที่ทำหน้าที่ติดต่อเป้าหมาย (2) กลุ่มสนับสนุนหรือผู้ดูแลระบบ และ (3) นายทุน การทำงานของมิจฉาชีพมีการหาข้อมูลเป็นอย่างดี ทันต่อเหตุการณ์ และปรับเปลี่ยนกลยุทธ์ได้อย่างรวดเร็ว

2. มิจฉาชีพมีการตั้งฐานปฏิบัติการในต่างประเทศและมีลักษณะเหมือนอาชญากรรมข้ามชาติ โดยเฉพาะในบริเวณชายแดนประเทศเพื่อนบ้านของไทย เนื่องจากกฎหมายไทยไม่สามารถบังคับใช้ได้ในต่างประเทศ ซึ่งในบริเวณนี้ ขบวนการมิจฉาชีพยังได้ประโยชน์จากความสะดวกในการเคลื่อนย้ายแรงงานและยังสามารถใช้สัญญาณโทรศัพท์เคลื่อนที่และอินเทอร์เน็ตของไทยได้

3. มิจฉาชีพสามารถจัดหาช่องทางและอุปกรณ์ต่าง ๆ ที่ใช้ในการสื่อสารเพื่อเข้าถึงเป้าหมายได้หลายวิธี โดยเฉพาะการใช้ซิมการ์ดหรือ “ซิมม้า” เพื่อปกปิดตัวตนและหลีกเลี่ยงข้อจำกัดในการลงทะเบียนซิมซึ่งเป็นแนวทางที่กำหนดโดยสำนักงาน กสทช.

4. มิจฉาชีพได้ใช้หลักการหลอกลวงทางจิตวิทยาต่าง ๆ เพื่อโจมตีจุดอ่อนของเป้าหมาย หลักการดังกล่าวเป็นหลักการในการโน้มน้าวจิตใจทางจิตวิทยา เช่น หลักการตอบสนองตามต้องการพื้นฐานของมนุษย์ (Visceral triggers) ซึ่งหลอกให้เป้าหมายรู้สึกอยากได้อยากมี หลอกให้เชื่อในอำนาจ (Authority) ของเจ้าหน้าที่ของรัฐ และ หลักการด้านเวลา (Time Principle) ซึ่งบีบบังคับให้เป้าหมายตัดสินใจในเวลาจำกัดซึ่งจะผิดพลาดได้ง่าย หลักการทางจิตวิทยาเหล่านี้ที่มักมุ่งเน้นไปที่จุดอ่อนของมนุษย์ ทำให้เกิดความผิดพลาดในระบบการตัดสินใจ (Error in judgement)

5. มิจฉาชีพได้ใช้ Mobile Banking และ “บัญชีม้า” ในการโยกย้ายทรัพย์สิน มิจฉาชีพมักใช้บัญชีม้าควบคู่กับ Mobile Banking เพื่อความรวดเร็วในการโยกย้ายทรัพยสิน อีกทั้งปลายทางของบัญชีมักมีการแปลงให้สินทรัพย์อยู่ในรูปแบบเงินสกุลดิจิทัลเพื่อให้ติดตามจับกุมได้ยาก

ผลกระทบของการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ต่อสังคมและผู้บริโภค

1. ผลกระทบต่อความอยู่ดีมีสุขของประชาชน ประชาชนจำนวนมากถูกหลอกและเสียทรัพย์สินให้กับมิจฉาชีพ และมีความเสียหายทางสุขภาพจิต มักรู้สึกอับอายและโทษตัวเองที่เสียรู้ให้กับมิจฉาชีพ นอกจากนี้ อาจมีการลบหรือบล็อกสายโทรเข้าหรือข้อความที่สำคัญไปอีกด้วย

2. ผลกระทบต่อผู้ประกอบการและหน่วยงานที่เกี่ยวข้อง หน่วยงานที่เกี่ยวข้องเกิดภาพลักษณ์ที่ไม่ดีต่อประชาชนทั้งจากการถูกแอบอ้างโดยมิจฉาชีพและจากความคาดหวังของประชาชน และหน่วยงานที่เกี่ยวข้องยังมีการสูญเสียทรัพยากรสำหรับการเตรียมระบบป้องกันมิจฉาชีพทั้งทรัพยากรด้านบุคลากร งบประมาณ และเวลา

3. ผลกระทบต่อสังคม ประชาชนที่รับรู้ข่าวสารอยู่ในภาวะวิตกกังวล และเกิดเป็นความหวาดระแวงต่อกันได้ กล่าวได้ว่าทำให้เกิดภาวะการไม่ไว้วางใจกันในสังคม

4. ผลกระทบต่อประเทศและความมั่นคง ผลกระทบต่อเศรษฐกิจของประเทศ เนื่องจากมิจฉาชีพจะถ่ายเททรัพย์สินออกนอกประเทศ และการที่ประชาชนได้รับผลกระทบต่อความอยู่ดีมีสุขยังพิจารณาได้ว่ากระทบต่อความมั่นคงของประเทศตามที่ได้กำหนดในยุทธศาสตร์ชาติ 20 ปี

การดำเนินการในปัจจุบันของหน่วยงานที่เกี่ยวข้อง

ปัจจุบันหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนได้มีมาตรการหรือแนวทางในการแก้ไขและป้องกันปัญหามากมาย โดยมุ่งเน้นทั้งในส่วนของผู้กระทำผิด ผู้เสียหาย และโอกาสหรือช่องทางของการกระทำผิด ซึ่งเป็นองค์ประกอบสำคัญ 3 ส่วนตามทฤษฎีสามเหลี่ยมอาชญากรรม และยังมีมาตรการที่เป็นภาพรวมของการแก้ไขและป้องกันปัญหา ดังนี้

1. ผู้กระทำผิด แนวทางในการแก้ไขปัญหาที่มุ่งเน้นในส่วนของผู้กระทำผิดจะเป็นการวางกรอบแนวทางให้สามารถจับกุมผู้กระทำความผิดได้ และยังเป็นการป้องปรามผู้ที่คิดจะกระทำผิด โดยได้มีการบังคับใช้ “พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี” เพื่อให้มีบทลงโทษครอบคลุมทุกกลุ่มของมิจฉาชีพ เช่น การซื้อขายบัญชีม้าและซิมม้า เป็นต้น

2. ผู้เสียหาย แนวทางในส่วนของผู้เสียหายจะมีทั้งแนวทางที่มุ่งเน้นในการแจ้งเตือนประชาชนผ่านระบบการแจ้งเตือนต่าง ๆ เพื่อให้ทราบว่ากำลังถูกคุกคามจากมิจฉาชีพ เช่น การเตือนผู้ใช้บริการเมื่อมีเลขหมายที่โทรมาจากต่างประเทศผ่าน VoIP โดยการใส่ Prefix “+697” และ “+698” การให้มี Sender name ของผู้ส่งข้อความสั้น (SMS) และการพัฒนาแอปพลิเคชัน “กันกวน” ของสำนักงาน กสทช. รวมทั้งยังมีการจัดทำฐานข้อมูลที่เป็นแหล่งความรู้ให้แก่ประชาชน เช่น การจัดทำฐานข้อมูลชื่อ “SCAM Alert/เท่าทันมิจฉาชีพ” ของสำนักงาน กสทช. นอกจากนี้ หน่วยงานต่าง ๆ ก็มีแนวทางในการช่วยเหลือผู้เสียหาย เช่น การอำนวยความสะดวกให้ผู้เสียหายสามารถแจ้งความร้องทุกข์ได้อย่างสะดวกและรวดเร็วผ่านช่องทางออนไลน์ที่ thaipoliceonline.com การกำหนดขั้นตอนการดำเนินการที่เกี่ยวข้องการระงับธุรกรรมทางการเงินต้องสงสัย และการจัดทำช่องทางการติดต่อ โดยหน่วยงานต่าง ๆ เช่น การดำเนินการของ ธปท. ซึ่งได้กำหนดให้ทุกธนาคารมีช่องทางติดต่อเร่งด่วน (hotline) ตลอด 24 ชั่วโมง

3. โอกาสและช่องทางของการกระทำผิด แนวทางในส่วนของโอกาสและช่องทางของการกระทำผิดจะมุ่งเน้นไปที่การตัดโอกาสในการเข้าถึงประชาชนของมิจฉาชีพตั้งแต่ต้น เพื่อลดความเสี่ยงจากการต้องใช้วิจารณญาณของประชาชนเมื่อต้องเผชิญกับมิจฉาชีพ จากการศึกษาวรรณกรรมที่เกี่ยวข้อง พบว่าการหลอกลวงของมิจฉาชีพได้โจมตีจุดอ่อนของมนุษย์ด้วยเทคนิคทางจิตวิทยา ทำให้เป้าหมายหลงกลได้ง่ายแม้ว่าจะเป็นผู้มีความรู้ความสามารถมากก็ตาม แนวทางในปัจจุบันของหน่วยงานต่าง ๆ เช่น สำนักงาน กสทช. ได้มีจัดทำบริการ USSD (Unstructured Supplementary Services Data) หมายเลข *138 เพื่อให้ผู้ใช้บริการสามารถเลือกปฏิเสธการรับสายที่เป็นทราฟฟิกจากต่างประเทศได้ เป็นต้น นอกจากการปิดกั้นโอกาสในการเข้าถึงเป้าหมายแล้ว ยังมีการปิดกั้นโอกาสในการโยกย้ายทรัพย์สินไปยังมือมิจฉาชีพด้วย โดย ธปท. ได้กำหนดให้มีการป้องกันมิให้มีช่องว่างในการใช้งานบัญชีและ Mobile banking ที่ทำให้มิจฉาชีพนำไปใช้ในการหลอกลวงได้

4. ในภาพรวมของมาตรการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้มีการกำหนดให้มีการแก้ปัญหาร่วมกันระหว่างหน่วยงานต่าง ๆ ได้แก่ สำนักงานตำรวจแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงาน กสทช. ผู้ให้บริการในกิจการโทรคมนาคม ธปท. และสถาบันการเงินต่าง ๆ ซึ่งก่อให้เกิดการดำเนินการแบบบูรณาการได้อีกด้วย

ข้อเสนอแนะเชิงนโยบายและมาตรการในการแก้ไขและป้องกันปัญหาการหลอกลวงผ่านเครือข่ายโทรศัพท์เคลื่อนที่ในประเทศไทย

จากการวิเคราะห์ช่องว่าง (Gap Analysis) ระหว่างแนวทางหรือมาตรการในปัจจุบันกับรูปแบบพฤติกรรมการหลอกลวงและเป้าหมายที่ตั้งไว้ พบว่ายังมีช่องว่างที่จะสามารถต่อยอด หรือปรับปรุง เพื่อให้สามารถแก้ไขและป้องกันปัญหาการหลอกลวงได้อย่างมีประสิทธิภาพมากขึ้น โดยข้อเสนอแนะในการแก้ไขและป้องกันปัญหาการหลอกลวง มีดังนี้

1. **ข้อเสนอแนะเชิงนโยบาย**

1.1 ควรมีการบังคับใช้กฎหมายที่มีอยู่เพื่อให้เกิดประโยชน์สูงสุด เช่น สนับสนุนให้มีการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอย่างจริงจัง ทั้งในเรื่องการจัดตั้งความร่วมมือของหน่วยงานต่าง ๆ ในกระบวนการจับกุม และการลงโทษผู้กระทำผิด

1.2 ปรับแก้กฎหมายให้มีบทลงโทษที่เหมาะสม โดยอาจมีการกำหนดอัตราโทษของผู้กระทำผิดซึ่งเดิมมีความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญาให้สูงขึ้น หรือปรับปรุงให้มีความเหมาะสมกับลักษณะของอาชญากรรมที่เปลี่ยนแปลงไป และให้สอดคล้องกับการลงโทษกลุ่มสนับสนุนมิจฉาชีพที่กำหนดไว้ในพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2. ข้อเสนอแนะเชิงปฏิบัติการ

2.1 สร้างความตระหนักรู้และให้ข้อมูลแก่ประชาชนอย่างครอบคลุมทุกกลุ่ม เช่น ควรมีการใช้สื่อประชาสัมพันธ์ที่หลากหลายมากขึ้น โดยคำนึงถึงข้อจำกัดในการเข้าถึงสื่อของประชาชนทุกกลุ่ม รวมทั้งผู้ด้อยโอกาสต่าง ๆ เพื่อให้ข้อมูลถูกส่งต่อไปยังประชาชนให้มากที่สุด

2.2 มีการเยียวยาสุขภาพจิตของผู้เสียหาย ควรมีการพิจารณาประเด็นเรื่องปัญหาสุขภาพจิตของผู้เสียหายจากการหลอกลวง เพื่อให้มีการจัดตั้งศูนย์เยียวยาและฟื้นฟูสุขภาพจิตของผู้เสียหายและผู้ที่เกี่ยวข้องกับผู้เสียหาย โดยต้องมีเจ้าหน้าที่ที่มีความชำนาญเฉพาะทางในการให้คำปรึกษา และสนับสนุนผู้เสียหายให้มีกำลังใจในการให้ข้อมูลที่จำเป็นต่อเจ้าหน้าที่ที่เกี่ยวข้อง

2.3 ควรจัดทำช่องทางการร้องเรียนที่เป็นศูนย์กลางของการร้องเรียน อาจพิจารณาการจัดตั้งช่องทางศูนย์กลางของทุกหน่วยงาน ในการติดต่อเฉพาะเรื่องปัญหาอาชญากรรมทางเทคโนโลยี

2.4 จัดตั้งความร่วมมือระหว่างประเทศในรูปแบบต่าง ๆ เพื่อให้สามารถจับกุมและปราบปรามการกระทำผิดที่เกิดขึ้นในต่างประเทศได้อย่างมีประสิทธิภาพ

2.5 ควรปรับปรุงระบบการแจ้งเตือนประชาชนเมื่อมีการติดต่อจากมิจฉาชีพโดยนำเทคโนโลยีต่าง ๆ มาใช้ โดยอาจมีการพิจารณานำระบบตรวจสอบตัวตนของผู้โทรมาใช้ ดังที่มีตัวอย่างการใช้ในต่างประเทศ เช่น CLI ของสหราชอาณาจักร หรือ STIR/SHAKEN ของสหรัฐอเมริกา

2.6 ควรจัดตั้งความร่วมมือแบบบูรณาการของหน่วยงานที่เกี่ยวข้องทั้งหมด อาจมีการจัดตั้งความร่วมมืออื่น ๆ เพิ่มเสริมการจัดตั้งคณะกรรมการของพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยต้องมีลักษณะเป็นการบูรณาการของภาคส่วนต่าง ๆ

3. ข้อเสนอแนะสำหรับงานวิจัยในอนาคต

ด้วยข้อจำกัดของงานวิจัยนี้ งานวิจัยต่อไปอาจพิจารณาการเก็บข้อมูลจากฝั่งผู้กระทำผิดและผู้เสียหาย นอกจากนี้ ควรมีศึกษาในเชิงลึกเกี่ยวกับเทคโนโลยี หรือระบบยืนยันตัวตนผู้โทร และการหลอกลวงรูปแบบใหม่ผ่านสื่อออนไลน์ต่าง ๆ ด้วย เพื่อให้มีข้อมูลและความเห็นที่รอบด้าน